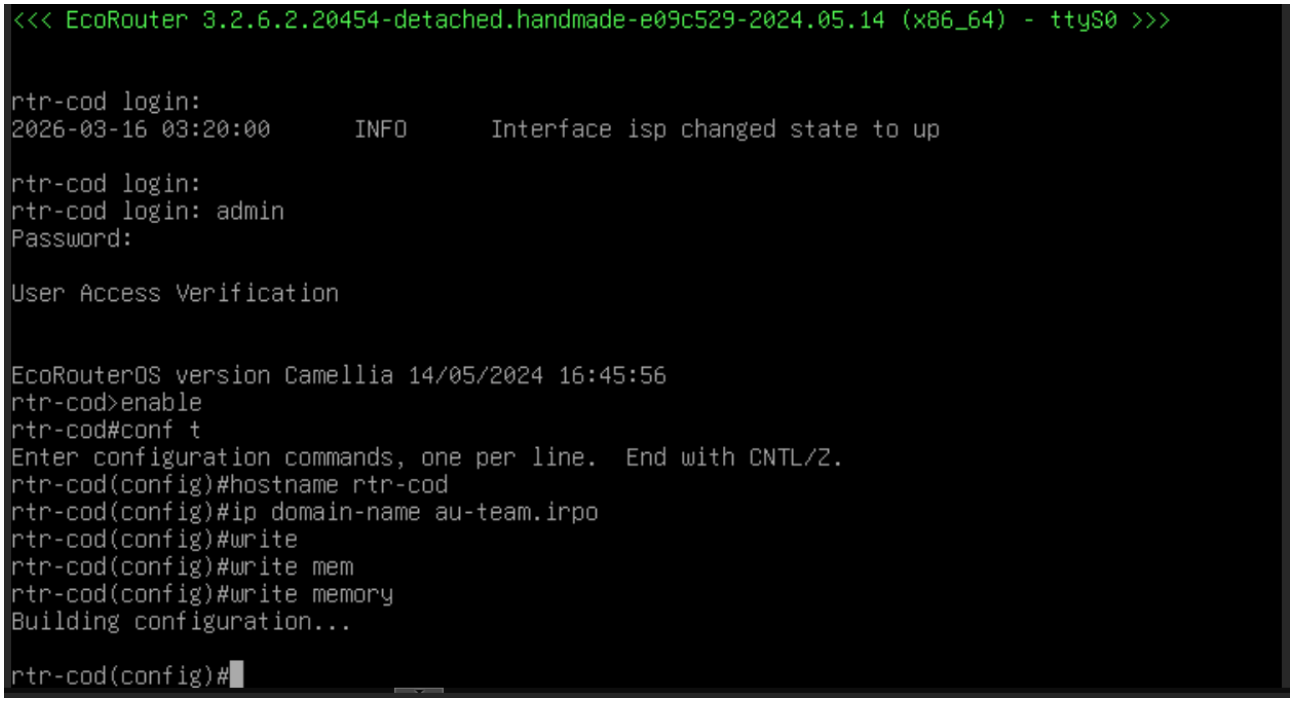
##########################ECOROUTER#######################################

login admin
password admin
enable
conf t
hostname rtr-cod - установка хостнейма
ip domain-name au.team - установка доменного имени
write memory



show port brief - просмотр физических портов

interface isp -создание интерфейса с именем isp
ip address 34.95.33.33/24 -адрес и маска устройства (интерфейса) которое настраиваем
decription "Connect for ISP" - description устанавливает подпись для интерфейса и не влияет на работу

show ip interface brief - проверка созданных интерфейсов

```
rtr-cod(config)#do show port brief
 Name            Physical   Admin   Lacp    Description
 ------------------------------------------------------------
 te0             UP         UP      *
 te1             UP         UP      *
rtr-cod(config)#interface isp
rtr-cod(config-if)#ip address 34.95.33.33/24
rtr-cod(config-if)#description "Connect for ISP"
rtr-cod(config-if)#ip inter
rtr-cod(config-if)#ip interf
rtr-cod(config-if)#ip interface brief
                   ^
% Invalid input detected at '^' marker.

rtr-cod(config-if)#do ip interface brief
                      ^
% Invalid input detected at '^' marker.

rtr-cod(config-if)#do show ip interface brief
 Interface       IP-Address          Status                VRF
 ------------------------------------------------------------
 isp             34.95.33.33/24      up                    default
 fw-cod          172.16.0.1/23       down                  default
rtr-cod(config-if)#
```

----НАСТРОЙКА ПОРТОВ И ПРИВЯЗЫВАНИЕ К НИМ ИНТЕРФЕЙСОВ----
port te0
service-instance te0/isp -связывание физического интерфейса te0 с интерфейсом isp (создание инстанса)
encapsulation untagged -не тегированный трафик(без VLAN)
connect ip interface isp

```
rtr-cod(config)#interface isp
rtr-cod(config-if)#ip address 34.95.33.33/24
rtr-cod(config-if)#description "Connect for ISP"
rtr-cod(config-if)#ip inter
rtr-cod(config-if)#ip interf
rtr-cod(config-if)#ip interface brief
                   ^
% Invalid input detected at '^' marker.

rtr-cod(config-if)#do ip interface brief
                      ^
% Invalid input detected at '^' marker.

rtr-cod(config-if)#do show ip interface brief
 Interface       IP-Address          Status                VRF
 ------------------------------------------------------------
 isp             34.95.33.33/24      up                    default
 fw-cod          172.16.0.1/23       down                  default
rtr-cod(config-if)#port te0
rtr-cod(config-port)#service-instance te0/isp
rtr-cod(config-service-instance)#encapsulation untagged
% Can't change encapsulation with connected service instance!
rtr-cod(config-service-instance)#connect ip interface isp
% Service instance is already connected
rtr-cod(config-service-instance)#
```

----НАСТРОЙКА МАРШРУТИЗАЦИИ----
ip route 0.0.0.0/0 34.95.33.1 -маршрутизация всех интерфейсов на 34.95.33.1

```
rtr-cod(config)#ip route 0.0.0.0/0 34.95.33.1
rtr-cod(config)#
```

----ПРОВЕРКА ДОСТУПА ВО ВНЕШНЮЮ СЕТЬ----

ping 1.1.1.1

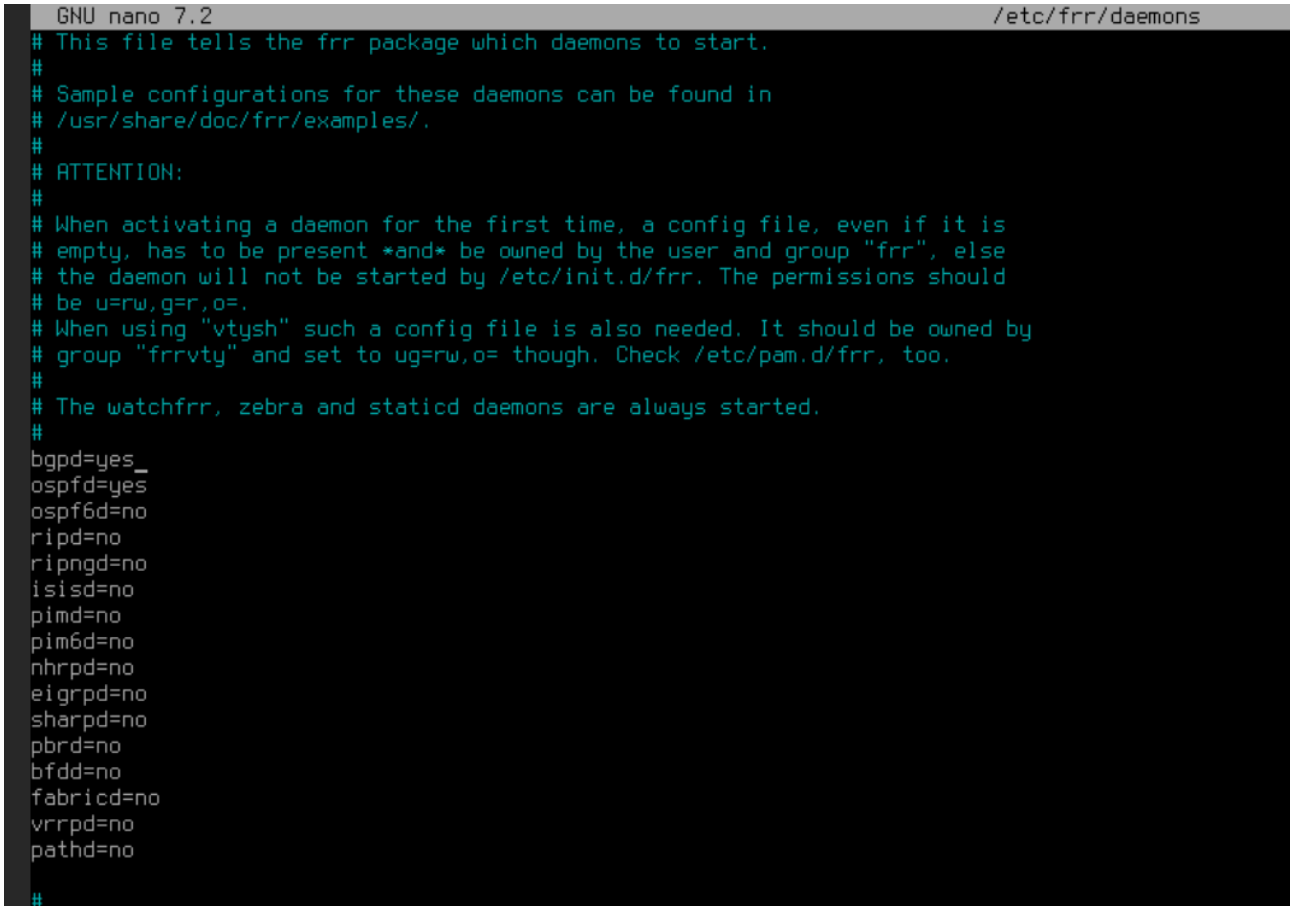
```
rtr-cod(config)#do ping 1.1.1.1
PING 1.1.1.1 (1.1.1.1) 56(84) bytes of data.
64 bytes from 1.1.1.1: icmp_seq=2 ttl=55 time=148 ms
64 bytes from 1.1.1.1: icmp_seq=3 ttl=55 time=94.3 ms
64 bytes from 1.1.1.1: icmp_seq=4 ttl=55 time=117 ms
64 bytes from 1.1.1.1: icmp_seq=5 ttl=55 time=59.5 ms
64 bytes from 1.1.1.1: icmp_seq=6 ttl=55 time=142 ms
64 bytes from 1.1.1.1: icmp_seq=7 ttl=55 time=125 ms
```

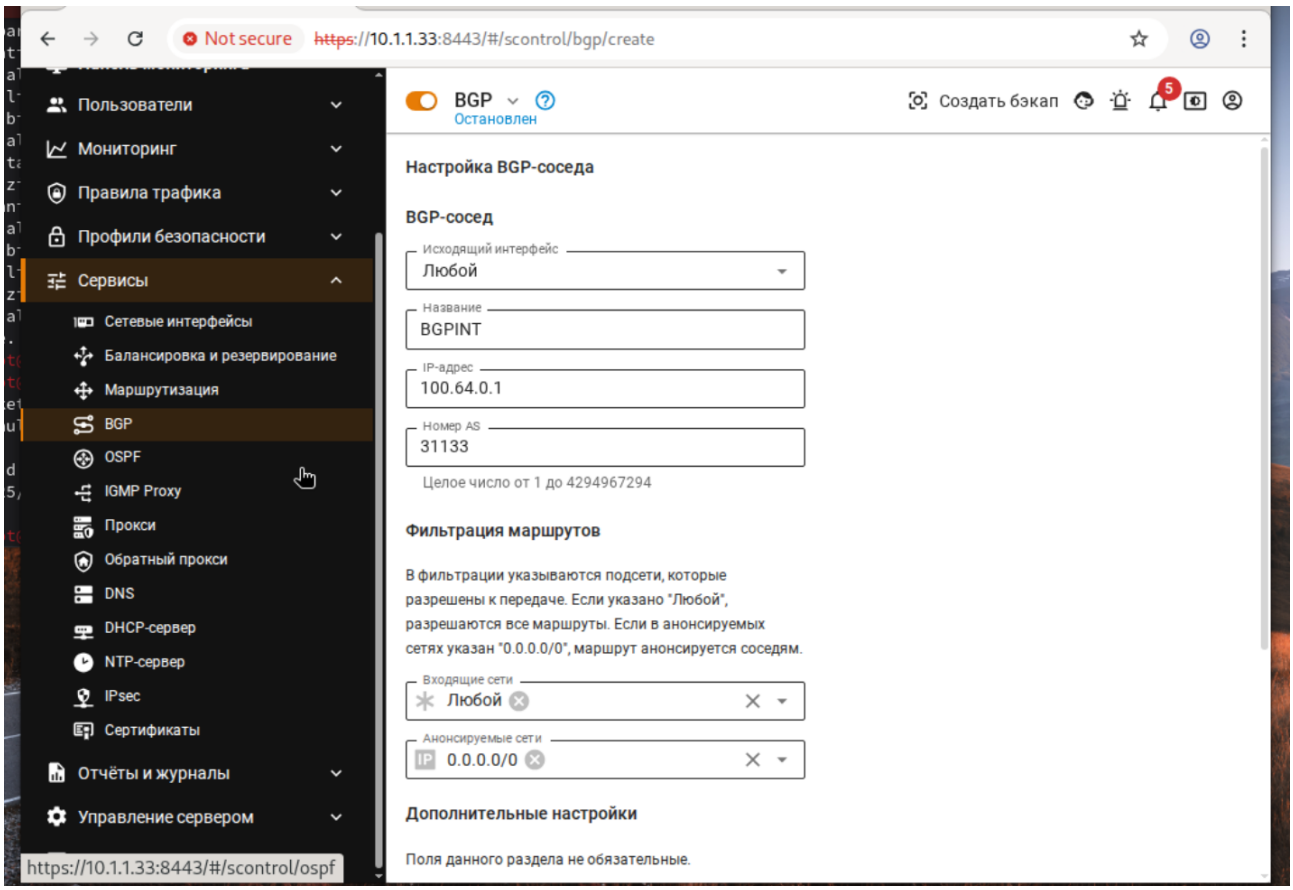
----СОЗДАНИЕ ПОЛЬЗОВАТЕЛЯ NET_ADMIN----

username net_admin
description sysadmin
password P@ssw0rd
role admin

```
rtr-cod>en
rtr-cod#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
rtr-cod(config)#username net_admin
rtr-cod(config-user)#description sysadmin
rtr-cod(config-user)#password P@ssw0rd
rtr-cod(config-user)#role admin
rtr-cod(config-user)#
```

----BGP HA FW-HQ----


GNU nano 7.2 /etc/frr/daemons
This file tells the frr package which daemons to start.
#
Sample configurations for these daemons can be found in
/usr/share/doc/frr/examples/.
#
ATTENTION:
#
When activating a daemon for the first time, a config file, even if it is
empty, has to be present *and* be owned by the user and group "frr", else
the daemon will not be started by /etc/init.d/frr. The permissions should
be u=rw,g=r,o=.
When using "vtysh" such a config file is also needed. It should be owned by
group "frrvty" and set to ug=rw,o= though. Check /etc/pam.d/frr, too.
#
The watchfrr, zebra and staticd daemons are always started.
#
bgpd=yes
ospfd=yes
ospf6d=no
ripd=no
ripngd=no
isisd=no
pimd=no
pim6d=no
nhrpd=no
eigrpd=no
sharpd=no
pbrd=no
bfdd=no
fabricd=no
vrrpd=no
pathd=no
#


Not secure
https://10.1.1.33:8443/#/scontrol/bgp/create
Пользователи
Мониторинг
Правила трафика
Профили безопасности
Сервисы
Сетевые интерфейсы
Балансировка и резервирование
Маршрутизация
BGP
OSPF
IGMP Proxy
Прокси
Обратный прокси
DNS
DHCP-сервер
NTP-сервер
IPsec
Сертификаты
Отчёты и журналы
Управление сервером
https://10.1.1.33:8443/#/scontrol/ospf
BGP
Остановлен
Создать бэкап
Настройка BGP-соседа
BGP-сосед
Исходящий интерфейс
Любой
Название
BGPINT
IP-адрес
100.64.0.1
Номер AS
31133
Целое число от 1 до 4294967294
Фильтрация маршрутов
В фильтрации указываются подсети, которые разрешены к передаче. Если указано "Любой", разрешаются все маршруты. Если в анонсируемых сетях указан "0.0.0.0/0", маршрут анонсируется соседям.
Входящие сети
Любой
Анонсируемые сети
0.0.0.0/0
Дополнительные настройки
Поля данного раздела не обязательные.

----НАСТРОЙКА BGP----

router bgp 64500
bgp router-id 100.64.0.3
neighbor 100.64.0.1 remote-as 31133
write memory

```
rtr-cod(config)#router bgp 64500
rtr-cod(config-router)#bgp router id 178.207.179.4
                              ^
% Invalid input detected at '^' marker.

rtr-cod(config-router)#bgp router-id 178.207.179.4
rtr-cod(config-router)#neighbor 178.207.179.1 remote-as 31133
rtr-cod(config-router)#write memory
Building configuration...
```

```
rtr-br(config)#router bgp 64500
rtr-br(config-router)#bgp router-id 100.64.0.3
rtr-br(config-router)#neighbor 100.64.0.1 remo
remote-as          remove-private-as
rtr-br(config-router)#neighbor 100.64.0.1 remote-as 64499
rtr-br(config-router)#write memory
Building configuration...

rtr-br(config-router)#
```

----GRE ТУННЕЛЬ----

interface tunnel.0
ip address 10.0.3.2/30
ip tunnel 84.212.78.78 34.95.33.33 mode gre (84.212.78.78 — rtr-br, 34.95.33.33 — rtr-cod)

RTR-BR
ip tunnel 84.212.78.78 34.95.33.33 mode gre (84.212.78.78 — rtr-br, 34.95.33.33 — rtr-cod)

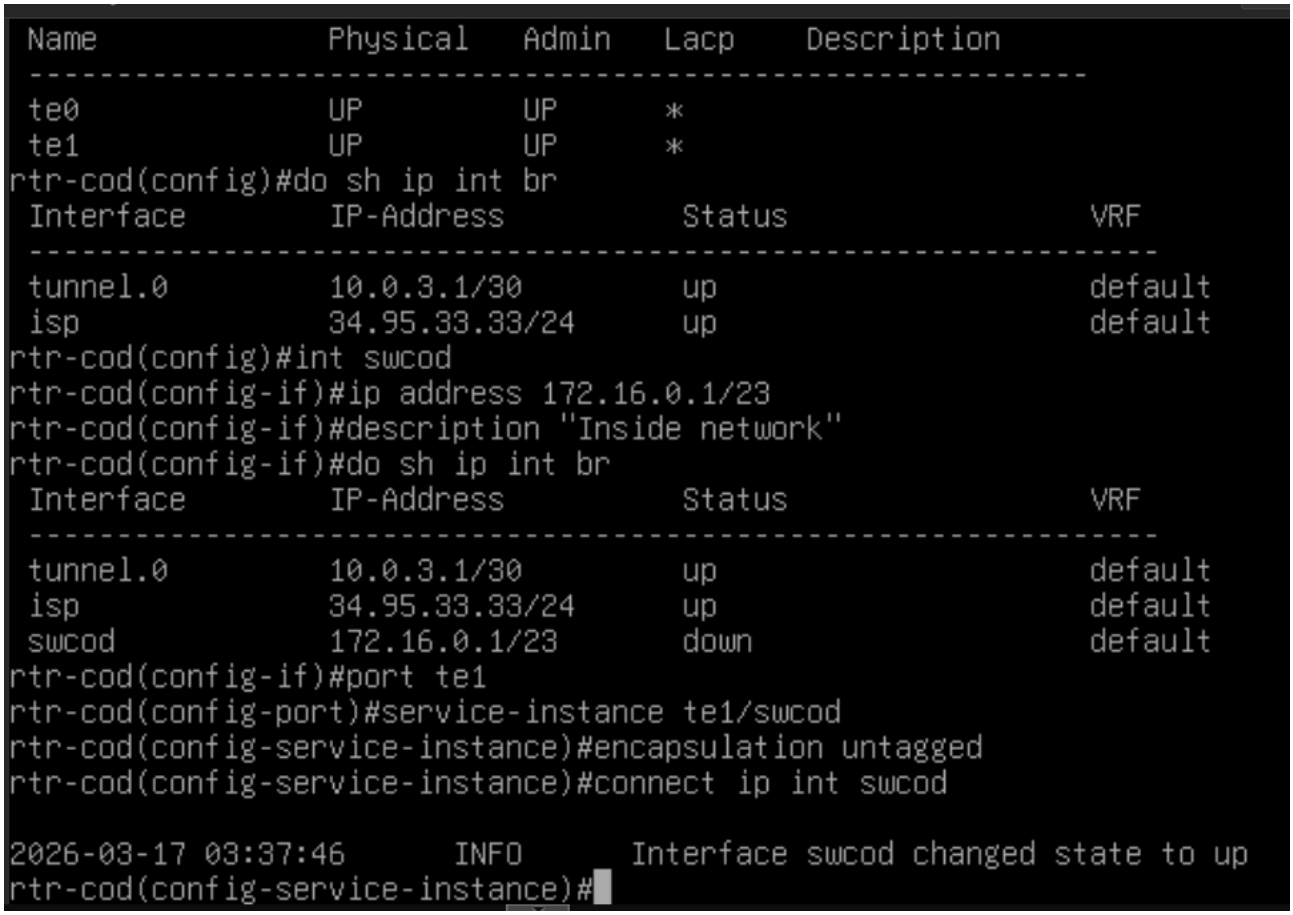
RTR-COD
ip tunnel 34.95.33.33 84.212.78.78 mode gre (84.212.78.78 — rtr-br, 34.95.33.33 — rtr-cod)

```
rtr-br(config)#int tunnel.0
rtr-br(config-if-tunnel)#ip address 10.0.3.2/30
rtr-br(config-if-tunnel)#ip tunnel ip tun
rtr-br(config-if-tunnel)#ip tunnel 84.212.78.78 34.95.33.33 mode gre

2026-03-16 07:50:36      INFO      Interface tunnel.0 changed state to up
rtr-br(config-if-tunnel)#do sh int tunnel.0
 Interface tunnel.0 is up
  Snmp index: 7
  Ethernet address: (port not configured)
  MTU: 1476
  Tunnel source: 84.212.78.78
  Tunnel destination: 34.95.33.33
  Tunnel mode: GRE
  NAT: no
  ARP Proxy: disable
  ICMP redirects on, unreachables on
  IP URPF is disabled
  Label switching is disabled
  <UP,BROADCAST,RUNNING,NOARP,MULTICAST>
  inet 10.0.3.2/30 broadcast 10.0.3.3/30
  total input packets 0, bytes 0
  total output packets 0, bytes 0
rtr-br(config-if-tunnel)#
```

```
  Snmp index: 7
  Ethernet address: (port not configured)
  MTU: 1476
  Tunnel source: 34.95.33.33
  Tunnel destination: 84.212.78.78
  Tunnel mode: GRE
  NAT: no
  ARP Proxy: disable
  ICMP redirects on, unreachables on
  IP URPF is disabled
  Label switching is disabled
  <UP,BROADCAST,RUNNING,NOARP,MULTICAST>
  inet 10.0.3.1/30 broadcast 10.0.3.3/30
  total input packets 0, bytes 0
  total output packets 0, bytes 0
rtr-cod(config-if-tunnel)#do ping 84.212.78.78
PING 84.212.78.78 (84.212.78.78) 56(84) bytes of data.
64 bytes from 84.212.78.78: icmp_seq=1 ttl=63 time=73.5 ms
64 bytes from 84.212.78.78: icmp_seq=2 ttl=63 time=28.9 ms
64 bytes from 84.212.78.78: icmp_seq=3 ttl=63 time=30.9 ms

--- 84.212.78.78 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 28.947/44.445/73.464/20.535 ms
rtr-cod(config-if-tunnel)#
```

NAT И ВНУТРЕННЯЯ СЕТЬ----

1) Настройка интерфейса локальной сети (на rtr-cod в сторону sw-cod)



2) Тоже самое на rtr-br (интерфейс смотрит в сторону fw-br)

```
rtr-br(config)#int fwbr
rtr-br(config-if)#ip address 10.2.0.1
% Incomplete command.

rtr-br(config-if)#ip address 10.2.0.1/30
rtr-br(config-if)#description "inside for FWBR"
rtr-br(config-if)#do sh ip int br
 Interface        IP-Address          Status                VRF
 ---------------------------------------------------------------
 tunnel.0         10.0.3.2/30         up                    default
 isp              84.212.78.78/24     up                    default
 fwbr             10.2.0.1/30         down                  default
rtr-br(config-if)#do sh port br
 Name             Physical   Admin   Lacp    Description
 ------------------------------------------------------------
 te0              UP         UP      *
 te1              UP         UP      *
rtr-br(config-if)#port te1
rtr-br(config-port)#service-instance te1/fwbr
rtr-br(config-service-instance)#encapsulation untagged
rtr-br(config-service-instance)#connect ip int fwbr

2026-03-17 03:46:08      INFO      Interface fwbr changed state to up
rtr-br(config-service-instance)#
```

3) на каждом маршрутизаторе прописываем write memory для сохранения настроек

RTR-BR

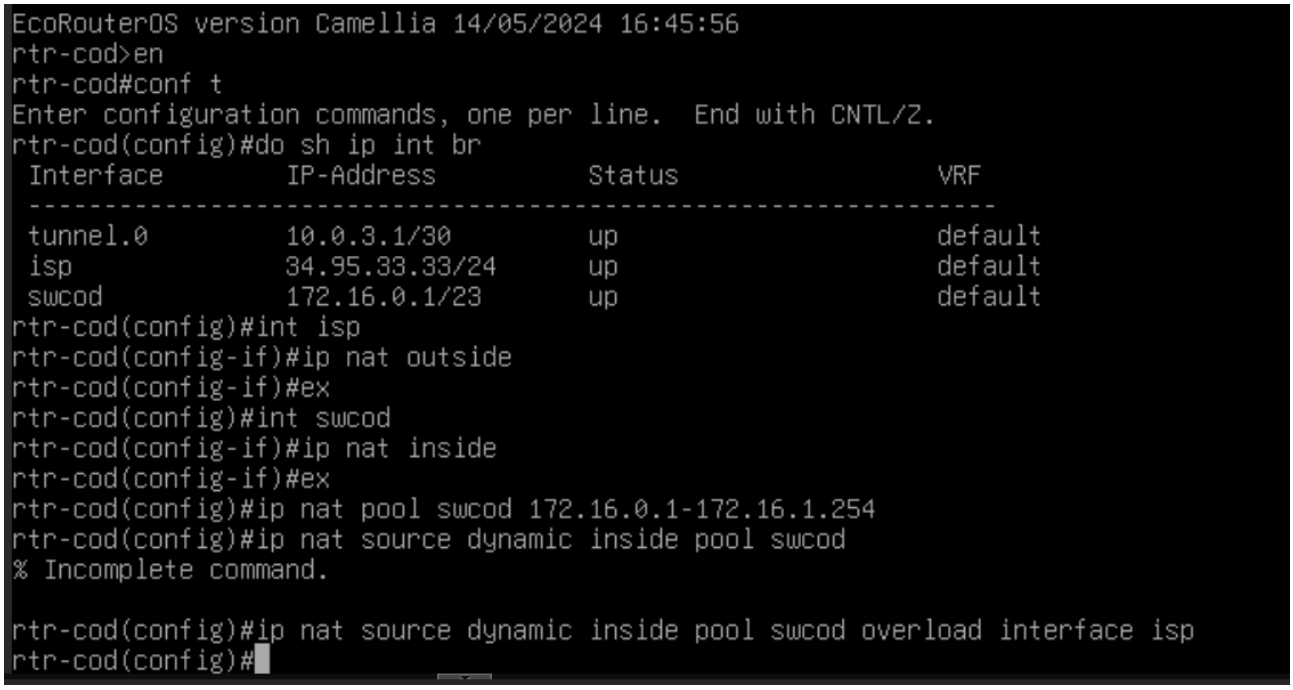
```
rtr-br(config-service-instance)#ex
rtr-br(config-port)#ex
rtr-br(config)#int isp
rtr-br(config-if)#ip nat outside
rtr-br(config-if)#ex
rtr-br(config)#do sh ip int br
 Interface        IP-Address          Status                VRF
 ---------------------------------------------------------------
 tunnel.0         10.0.3.2/30         up                    default
 isp              84.212.78.78/24     up                    default
 fwbr             10.2.0.1/30         up                    default
rtr-br(config)#int fwbr
rtr-br(config-if)#ip nat inside
rtr-br(config-if)#ex
rtr-br(config)#ip nat pool fwbr 10.2.0.1-10.2.0.2
rtr-br(config)#ip nat pool vlan10 10.1.1.1-10.1.1.30
rtr-br(config)#ip nat pool vlan20 10.1.1.33-10.1.1.47
rtr-br(config)#ip nat pool vlan30 10.1.2.1-10.1.2.254
rtr-br(config)#ip nat source dynamic inside pool fw
rtr-br(config)#ip nat source dynamic inside pool fwbr overload interface isp
rtr-br(config)#ip nat source dynamic inside pool vlan10 overload interface isp
rtr-br(config)#ip nat source dynamic inside pool vlan20 overload interface isp
rtr-br(config)#ip nat source dynamic inside pool vlan30 overload interface isp
rtr-br(config)#
```

interface isp
ip nat outside -интерфейс смотрящий в сторону ISP

interface fwbr

ip nat inside -интерфейс смотрящий «внутрь» т. е. в локальную сеть маршрутизатора

RTR-COD



isp — внешняя сеть (ip nat outside)

swcod — внутренняя сеть (ip nat inside)

Поскольку sw-cod это коммутатор согласно заданию то дополнительные интерфейсы не назначаем

###############SW-COD##############
login: root
passwd: toor or P@ssw0rd

echo «nameserver 8.8.8.8» >> /etc/resolv.conf
echo «172.16.1.2/23» >> /etc/net/ifaces/ens18/ipv4address
echo «default via 172.16.0.1» >> /etc/net/ifaces/ens18/ipv4route

Также в файле /etc/net/ifaces/ens18/options меняем параметры BOOTPROTO и SYSTEMD_BOOTPROTO на static

nameserver — указание DNS сервера
ipv4address — адрес sw-cod для подключения к rtr-cod
ipv4route шлюз для sw-cod т. е. Маршрутизатор rtr-cod

```
[root@host-83 ens18]# pwd
/etc/net/ifaces/ens18
[root@host-83 ens18]# cat options
BOOTPROTO=static
TYPE=eth
SYSTEMD_CONTROLLED=no
DISABLED=no
CONFIG_WIRELESS=no
SYSTEMD_BOOTPROTO=static
CONFIG_IPV4=yes
NM_CONTROLLED=no
[root@host-83 ens18]# cat ipv4address
172.16.1.2/23
[root@host-83 ens18]# cat ipv4route
default via 172.16.0.1
[root@host-83 ens18]# ip -c a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host proto kernel_lo
       valid_lft forever preferred_lft forever
2: ens18: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether bc:24:11:56:1c:ef brd ff:ff:ff:ff:ff:ff
    altname enp0s18
    inet 172.16.1.2/23 brd 172.16.1.255 scope global ens18
       valid_lft forever preferred_lft forever
    inet6 fe80::be24:11ff:fe56:1cef/64 scope link proto kernel_ll
       valid_lft forever preferred_lft forever
3: ens19: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ether bc:24:11:87:15:62 brd ff:ff:ff:ff:ff:ff
    altname enp0s19
4: ens20: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ether bc:24:11:e1:61:45 brd ff:ff:ff:ff:ff:ff
    altname enp0s20
5: ens21: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ether bc:24:11:f4:c0:25 brd ff:ff:ff:ff:ff:ff
    altname enp0s21
6: ens22: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ether bc:24:11:5b:54:c5 brd ff:ff:ff:ff:ff:ff
    altname enp0s22
7: ens23: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ether bc:24:11:00:33:a2 brd ff:ff:ff:ff:ff:ff
    altname enp0s23
[root@host-83 ens18]#
```

hostnamectl set-hostname sw-cod.au.team; exec bash

```
[root@host-83 ens18]# hostnamectl set-hostname sw-cod.au.team; exec bash
[root@sw-cod ens18]# _
```

----НАСТРОЙКА КОММУТАЦИИ----

Обновим и установим пакет openvswitch

```
[root@sw-cod ens18]# apt-get update && apt-get install openvswitch -y
```

systemctl enable —now openvswitch

```
Done.
[root@sw-cod ens18]# systemctl enable --now openvswitch.service
Synchronizing state of openvswitch.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable openvswitch
Created symlink /etc/systemd/system/multi-user.target.wants/openvswitch.service → /usr/lib/systemd/system/openvswitch.service.
[root@sw-cod ens18]#
```

создаем папки и копируем файл options

```
    link/ether bc:24:11:87:15:62 brd ff:ff:ff:ff:ff:ff
    altname enp0s19
4: ens20: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ether bc:24:11:e1:61:45 brd ff:ff:ff:ff:ff:ff
    altname enp0s20
5: ens21: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ether bc:24:11:f4:c0:25 brd ff:ff:ff:ff:ff:ff
    altname enp0s21
6: ens22: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ether bc:24:11:5b:54:c5 brd ff:ff:ff:ff:ff:ff
    altname enp0s22
7: ens23: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ether bc:24:11:00:33:a2 brd ff:ff:ff:ff:ff:ff
    altname enp0s23
[root@sw-cod ifaces]# mkdir ens19
[root@sw-cod ifaces]# mkdir ens2{0,1,2,3}
[root@sw-cod ifaces]# ls
default  ens18  ens19  ens20  ens21  ens22  ens23  lo  unknown
[root@sw-cod ifaces]# cd ens18
[root@sw-cod ens18]# ls
ipv4address  ipv4route  options
[root@sw-cod ens18]# cp options ../ens19
[root@sw-cod ens18]# cp options ../ens2{0,1,2,3}/
cp: -r not specified; omitting directory '../ens20/'
cp: -r not specified; omitting directory '../ens21/'
cp: -r not specified; omitting directory '../ens22/'
[root@sw-cod ens18]# ls ../ens20
[root@sw-cod ens18]# cp options ../ens2{0,1,2,3}
cp: overwrite '../ens23/options'? y
cp: -r not specified; omitting directory '../ens20'
cp: -r not specified; omitting directory '../ens21'
cp: -r not specified; omitting directory '../ens22'
[root@sw-cod ens18]# ls ../ens20
[root@sw-cod ens18]# cp options ../ens19
cp: overwrite '../ens19/options'? y
[root@sw-cod ens18]# cp options ../ens20
[root@sw-cod ens18]# cp options ../ens21
[root@sw-cod ens18]# cp options ../ens22
[root@sw-cod ens18]# cp options ../ens23
cp: overwrite '../ens23/options'? y
[root@sw-cod ens18]# cat options
BOOTPROTO=static
TYPE=eth
SYSTEMD_CONTROLLED=no
DISABLED=no
CONFIG_WIRELESS=no
SYSTEMD_BOOTPROTO=static
CONFIG_IPV4=yes
NM_CONTROLLED=no
[root@sw-cod ens18]#
```

Перезагружаем сеть и проверяем интерфейсы

systemctl restart network

ip -c -br a

```
[root@sw-cod ens18]# ip -c -br a
lo               UNKNOWN        127.0.0.1/8 ::1/128
ens18            UP             172.16.1.2/23 fe80::be24:11ff:fe56:1cef/64
ens19            UP             fe80::be24:11ff:fe87:1562/64
ens20            UP             fe80::be24:11ff:fee1:6145/64
ens21            UP             fe80::be24:11ff:fef4:c025/64
ens22            UP             fe80::be24:11ff:fe5b:54c5/64
ens23            UP             fe80::be24:11ff:fe00:33a2/64
[root@sw-cod ens18]#
```

создаем папку MGMT по пути /etc/net/ifaces и прописываем в ней файл options

```
[root@sw-cod MGMT]# pwd
/etc/net/ifaces/MGMT
[root@sw-cod MGMT]# ls
options
[root@sw-cod MGMT]# cat options
TYPE=ovsport
BOOTPROTO=static
CONFIG_IPV4=yes
BRIDGE=SW1-HQ
VID=0
[root@sw-cod MGMT]#
```

----OVS-SWITCH НАСТРОЙКА----

```
[root@sw-cod MGMT]# ovs-vsctl add-br SW-HQ
[root@sw-cod MGMT]# ovs-vsctl show
3110094b-c10a-4d1a-a532-85cc536ab7ae
    Bridge SW-HQ
        Port SW-HQ
            Interface SW-HQ
                type: internal
    ovs_version: "3.3.8"
[root@sw-cod MGMT]# sed -i "s/OVS_REMOVE=yes/OVS_REMOVE=no/g" /etc/net/ifaces/default/options
[root@sw-cod MGMT]# cd ../ens18
[root@sw-cod ens18]# ls
ipv4address  ipv4route  options
[root@sw-cod ens18]# mv ipv4address ../MGMT/
[root@sw-cod ens18]# mv ipv4route ../MGMT/
[root@sw-cod ens18]# systemctl restart network
[root@sw-cod ens18]# ip -c -br a
lo               UNKNOWN        127.0.0.1/8 ::1/128
ens18            UP             fe80::be24:11ff:fe56:1cef/64
ens19            UP             fe80::be24:11ff:fe87:1562/64
ens20            UP             fe80::be24:11ff:fee1:6145/64
ens21            UP             fe80::be24:11ff:fef4:c025/64
ens22            UP             fe80::be24:11ff:fe5b:54c5/64
ens23            UP             fe80::be24:11ff:fe00:33a2/64
ovs-system       DOWN
SW-HQ            DOWN
MGMT             UNKNOWN        172.16.1.2/23 fe80::a404:43ff:fe85:82ac/64
[root@sw-cod ens18]# ip -c -br -4 a
lo               UNKNOWN        127.0.0.1/8
MGMT             UNKNOWN        172.16.1.2/23
[root@sw-cod ens18]# _
```

SW-HQ — имя нашего бриджа указанного в /etc/net/ifaces/MGMT/options в параметре BRIDGE

Проверяем созданный бридж

```
[root@sw-cod ens18]# ovs-vsctl show
3110094b-c10a-4d1a-a532-85cc536ab7ae
    Bridge SW-HQ
        Port SW-HQ
            Interface SW-HQ
                type: internal
        Port MGMT
            tag: 0
            Interface MGMT
                type: internal
    ovs_version: "3.3.8"
[root@sw-cod ens18]#
```

Прописываем транки чтобы трафик шел без проблем

```
[root@sw-cod ens18]# ovs-vsctl add-port SW-HQ ens18 trunk=0
[root@sw-cod ens18]# ovs-vsctl add-port SW-HQ ens19 trunk=0
[root@sw-cod ens18]# ovs-vsctl add-port SW-HQ ens20 trunk=0
[root@sw-cod ens18]# ovs-vsctl add-port SW-HQ ens21 trunk=0
[root@sw-cod ens18]# ovs-vsctl add-port SW-HQ ens22 trunk=0
[root@sw-cod ens18]# ovs-vsctl add-port SW-HQ ens23 trunk=0
[root@sw-cod ens18]# ovs-vsctl show
3110094b-c10a-4d1a-a532-85cc536ab7ae
    Bridge SW-HQ
        Port ens23
            trunks: [0]
            Interface ens23
        Port ens21
            trunks: [0]
            Interface ens21
        Port ens18
            trunks: [0]
            Interface ens18
        Port SW-HQ
            Interface SW-HQ
                type: internal
        Port ens20
            trunks: [0]
            Interface ens20
        Port ens19
            trunks: [0]
            Interface ens19
        Port MGMT
            tag: 0
            Interface MGMT
                type: internal
        Port ens22
            trunks: [0]
            Interface ens22
    ovs_version: "3.3.8"
[root@sw-cod ens18]#
```

Включаем модуль 8021q и проверяем его наличие

```
[root@sw-cod ens18]# modprobe 8021q
[root@sw-cod ens18]# echo "8021q" | tee -a /etc/modules
8021q
[root@sw-cod ens18]# lsmod | grep "8021q"
8021q                  49152  0
garp                   16384  1 8021q
mrp                    20480  1 8021q
[root@sw-cod ens18]#
```

----НАСТРОЙКА IP АДРЕСАЦИИ НА ОСТАЛЬНЫХ УСТРОЙСТВАХ ЗОНЫ COD----

COD-SRV1:

Также меняем dhcp и dhcpd4 в файле options на static (файл находится по пути /etc/net/ifaces/ens18, вместо ens18 пишем имя нашего интерфейса)

```
[root@host-83 ~]# cd /etc/net/ifaces/ens18/
[root@host-83 ens18]# ls
options
[root@host-83 ens18]# echo "172.16.1.3/23" > ipv4address
[root@host-83 ens18]# echo "default via 172.16.0.1" > ipv4route
[root@host-83 ens18]# systemctl restart network
[root@host-83 ens18]# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host proto kernel_lo
       valid_lft forever preferred_lft forever
2: ens18: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether bc:24:11:48:c2:14 brd ff:ff:ff:ff:ff:ff
    altname enp0s18
    inet 172.16.1.3/23 brd 172.16.1.255 scope global ens18
       valid_lft forever preferred_lft forever
    inet6 fe80::be24:11ff:fe48:c214/64 scope link tentative proto kernel_ll
       valid_lft forever preferred_lft forever
[root@host-83 ens18]# ping 1.1.1.1
PING 1.1.1.1 (1.1.1.1) 56(84) bytes of data.
64 bytes from 1.1.1.1: icmp_seq=1 ttl=51 time=66.9 ms
64 bytes from 1.1.1.1: icmp_seq=2 ttl=51 time=47.9 ms
64 bytes from 1.1.1.1: icmp_seq=3 ttl=51 time=47.5 ms
^C
--- 1.1.1.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 47.524/54.109/66.903/9.048 ms
[root@host-83 ens18]#
```

default via 172.16.0.1 для всех оконченых устройств COD одинаковый

SRV2-COD:

```
Welcome to ALT Server 11.0 (Mendelevium)!

Hostname: host-83
IP: 127.0.0.2
host-83 login: root
Password:
Last login: Tue Feb 17 12:34:31 MSK 2026 on tty1
[root@host-83 ~]# hostnamectl set-hostname srv1-cod.au.team; exec bash
[root@srv1-cod ~]# ip -c a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: ens18: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether bc:24:11:d2:a2:d2 brd ff:ff:ff:ff:ff:ff
    altname enp0s18
    inet6 fe80::be24:11ff:fed2:a2d2/64 scope link proto kernel_ll
       valid_lft forever preferred_lft forever
[root@srv1-cod ~]# echo "default via 172.16.0.1" /etc/net/ifaces/ens18/ipv4route
default via 172.16.0.1 /etc/net/ifaces/ens18/ipv4route
[root@srv1-cod ~]# echo "default via 172.16.0.1" > /etc/net/ifaces/ens18/ipv4route
[root@srv1-cod ~]# echo "172.16.1.4/23" > /etc/net/ifaces/ens18/ipv4address
[root@srv1-cod ~]#
```

```
 GNU nano 8.0                                  /etc/net/ifaces/ens18/options
BOOTPROTO=static
TYPE=eth
SYSTEMD_CONTROLLED=no
DISABLED=no
CONFIG_WIRELESS=no
SYSTEMD_BOOTPROTO=static
CONFIG_IPV4=yes
NM_CONTROLLED=no
```

```
[root@srv1-cod ~]# systemctl restart network
[root@srv1-cod ~]# ip -c a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host proto kernel_lo
       valid_lft forever preferred_lft forever
2: ens18: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether bc:24:11:d2:a2:d2 brd ff:ff:ff:ff:ff:ff
    altname enp0s18
    inet 172.16.1.4/23 brd 172.16.1.255 scope global ens18
       valid_lft forever preferred_lft forever
    inet6 fe80::be24:11ff:fed2:a2d2/64 scope link proto kernel_ll
       valid_lft forever preferred_lft forever
[root@srv1-cod ~]# ping 1.1.1.1
PING 1.1.1.1 (1.1.1.1) 56(84) bytes of data.
64 bytes from 1.1.1.1: icmp_seq=1 ttl=54 time=57.7 ms
64 bytes from 1.1.1.1: icmp_seq=2 ttl=54 time=42.5 ms
64 bytes from 1.1.1.1: icmp_seq=3 ttl=54 time=44.2 ms
64 bytes from 1.1.1.1: icmp_seq=4 ttl=54 time=44.2 ms
^C
--- 1.1.1.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 42.471/47.138/57.736/6.157 ms
[root@srv1-cod ~]#
```

SRV3-COD:

```
Last login: Tue Feb 17 12:34:31 MSK 2026 on tty1
[root@host-83 ~]# hostnamectl set-hostname srv3-cod; exec bash
[root@srv3-cod ~]# ip -c a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: ens18: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether bc:24:11:8b:d2:f8 brd ff:ff:ff:ff:ff:ff
    altname enp0s18
    inet6 fe80::be24:11ff:fe8b:d2f8/64 scope link proto kernel_ll
       valid_lft forever preferred_lft forever
[root@srv3-cod ~]# echo "172.16.1.5/23" > /etc/net/ifaces/ens18/ipv4address
[root@srv3-cod ~]# echo "default via 172.16.0.1" > /etc/net/ifaces/ens18/ipv4route
[root@srv3-cod ~]#
```

```
 GNU nano 8.0                                  /etc/net/ifaces/ens18/options
BOOTPROTO=static
TYPE=eth
SYSTEMD_CONTROLLED=no
DISABLED=no
CONFIG_WIRELESS=no
SYSTEMD_BOOTPROTO=static
CONFIG_IPV4=yes
NM_CONTROLLED=no
```

```
[root@srv3-cod ~]# systemctl restart network
[root@srv3-cod ~]# ip -c a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host proto kernel_lo
       valid_lft forever preferred_lft forever
2: ens18: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether bc:24:11:8b:d2:f8 brd ff:ff:ff:ff:ff:ff
    altname enp0s18
    inet 172.16.1.5/23 brd 172.16.1.255 scope global ens18
       valid_lft forever preferred_lft forever
    inet6 fe80::be24:11ff:fe8b:d2f8/64 scope link proto kernel_ll
       valid_lft forever preferred_lft forever
[root@srv3-cod ~]# ping 1.1.1.1
PING 1.1.1.1 (1.1.1.1) 56(84) bytes of data.
64 bytes from 1.1.1.1: icmp_seq=1 ttl=51 time=132 ms
64 bytes from 1.1.1.1: icmp_seq=2 ttl=51 time=68.7 ms
64 bytes from 1.1.1.1: icmp_seq=3 ttl=51 time=123 ms
64 bytes from 1.1.1.1: icmp_seq=4 ttl=51 time=147 ms
^C
--- 1.1.1.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 68.733/117.766/147.191/29.617 ms
[root@srv3-cod ~]#
```

HA2-COD:

```
[root@host-83 ~]# hostnamectl set-hostname ha2-cod.au.team; exec bash
[root@ha2-cod ~]# ip -c a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: ens18: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether bc:24:11:c2:b7:4a brd ff:ff:ff:ff:ff:ff
    altname enp0s18
    inet6 fe80::be24:11ff:fec2:b74a/64 scope link proto kernel_ll
       valid_lft forever preferred_lft forever
[root@ha2-cod ~]# echo "172.16.1.6/23" > /etc/net/ifaces/ens18/ipv4address
[root@ha2-cod ~]# echo "default via 172.16.0.1" > /etc/net/ifaces/ens18/ipv4route
[root@ha2-cod ~]#
```

```
 GNU nano 8.0                                        /etc/net/ifaces/ens18/options
BOOTPROTO=static
TYPE=eth
SYSTEMD_CONTROLLED=no
DISABLED=no
CONFIG_WIRELESS=no
SYSTEMD_BOOTPROTO=static
CONFIG_IPV4=yes
NM_CONTROLLED=no
```

```
[root@ha2-cod ~]# systemctl restart network
[root@ha2-cod ~]# ip -c a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host proto kernel_lo
       valid_lft forever preferred_lft forever
2: ens18: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether bc:24:11:c2:b7:4a brd ff:ff:ff:ff:ff:ff
    altname enp0s18
    inet 172.16.1.6/23 brd 172.16.1.255 scope global ens18
       valid_lft forever preferred_lft forever
    inet6 fe80::be24:11ff:fec2:b74a/64 scope link proto kernel_ll
       valid_lft forever preferred_lft forever
[root@ha2-cod ~]# ping 1.1.1.1
PING 1.1.1.1 (1.1.1.1) 56(84) bytes of data.
64 bytes from 1.1.1.1: icmp_seq=1 ttl=54 time=52.2 ms
64 bytes from 1.1.1.1: icmp_seq=2 ttl=54 time=44.8 ms
64 bytes from 1.1.1.1: icmp_seq=3 ttl=54 time=43.6 ms
64 bytes from 1.1.1.1: icmp_seq=4 ttl=54 time=43.1 ms
^C
--- 1.1.1.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 43.131/45.734/52.204/3.746 ms
[root@ha2-cod ~]#
```

HA1-COD:

```
Last login: Tue Feb 17 12:34:31 MSK 2026 on tty1
[root@host-83 ~]# hostnamectl set-hostname ha1-cod; exec bash
[root@ha1-cod ~]# ip -c a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: ens18: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether bc:24:11:ec:59:db brd ff:ff:ff:ff:ff:ff
    altname enp0s18
    inet6 fe80::be24:11ff:feec:59db/64 scope link proto kernel_ll
       valid_lft forever preferred_lft forever
[root@ha1-cod ~]# echo "default via 172.16.0.1" > /etc/net/ifaces/ens18/ipv4route
[root@ha1-cod ~]# echo "172.16.1.7/23" > /etc/net/ifaces/ens18/ipv4address
[root@ha1-cod ~]#
```

```
BOOTPROTO=static
TYPE=eth
SYSTEMD_CONTROLLED=no
DISABLED=no
CONFIG_WIRELESS=no
SYSTEMD_BOOTPROTO=static
CONFIG_IPV4=yes
NM_CONTROLLED=no
```

```
[root@ha1-cod ~]# systemctl restart network
[root@ha1-cod ~]#
```

----SW-COD----

Создание учетной записи net_admin с паролем P@ssw0rd и правами рута

```
[root@sw-cod ~]# useradd
Usage: useradd [options] LOGIN
       useradd -D
       useradd -D [options]

Options:
  -b, --base-dir BASE_DIR       base directory for the home directory of the
                                new account
      --btrfs-subvolume-home    use BTRFS subvolume for home directory
  -c, --comment COMMENT         GECOS field of the new account
  -d, --home-dir HOME_DIR       home directory of the new account
  -D, --defaults                print or change default useradd configuration
  -e, --expiredate EXPIRE_DATE  expiration date of the new account
  -f, --inactive INACTIVE       password inactivity period of the new account
  -F, --add-subids-for-system   add entries to subuid/id even when adding a system user
  -g, --gid GROUP               name or ID of the primary group of the new
                                account
  -G, --groups GROUPS           list of supplementary groups of the new
                                account
  -h, --help                    display this help message and exit
  -k, --skel SKEL_DIR           use this alternative skeleton directory
  -K, --key KEY=VALUE           override /etc/login.defs defaults
  -m, --create-home             create the user's home directory
  -M, --no-create-home          do not create the user's home directory
  -N, --no-user-group           do not create a group with the same name as
                                the user
  -o, --non-unique              allow to create users with duplicate
                                (non-unique) UID
  -p, --password PASSWORD       encrypted password of the new account
  -r, --system                  create a system account
  -R, --root CHROOT_DIR         directory to chroot into
  -P, --prefix PREFIX_DIR       prefix directory where are located the /etc/* files
  -s, --shell SHELL             login shell of the new account
  -u, --uid UID                 user ID of the new account
  -U, --user-group              create a group with the same name as the user
  -Z, --selinux-user SEUSER     use a specific SEUSER for the SELinux user mapping
      --selinux-range SERANGE   use a specific MLS range for the SELinux user mapping

[root@sw-cod ~]# useradd -m -u 1010 -s /bin/bash net_admin
[root@sw-cod ~]# id
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel),19(proc)
[root@sw-cod ~]# usermod -aG root net_admin
[root@sw-cod ~]# usermod -aG wheel net_admin
[root@sw-cod ~]# apt-get install sudo -y
```

```
[root@sw-cod ~]# apt-get install sudo -y
Reading Package Lists... Done
Building Dependency Tree... Done
The following packages will be upgraded
  sudo
1 upgraded, 0 newly installed, 0 removed and 138 not upgraded.
Need to get 1274kB of archives.
After unpacking 4056B of additional disk space will be used.
Get:1 http://ftp.altlinux.org p11/branch/x86_64/classic sudo 1:1.9.16p2-alt3:p11+388680.100.1.1@1751397568 [1274kB]
Fetched 1274kB in 0s (2190kB/s)
Committing changes...
Preparing...                                    ################################################################################
Updating / installing...
1: sudo-1:1.9.16p2-alt3                         ################################################################################
Cleaning up / removing...
2: sudo-1:1.9.16p2-alt2                         ################################################################################
Done.
[root@sw-cod ~]# nano /etc/sudoers
```

в конец файла добавляем следующую строку и сохраняем

```
net_admin ALL=(ALL:ALL) NOPASSWD: ALL
```

ставим пароль на пользователя net_admin для авторизации в системе (пароль P@ssw0rd согласно заданию)

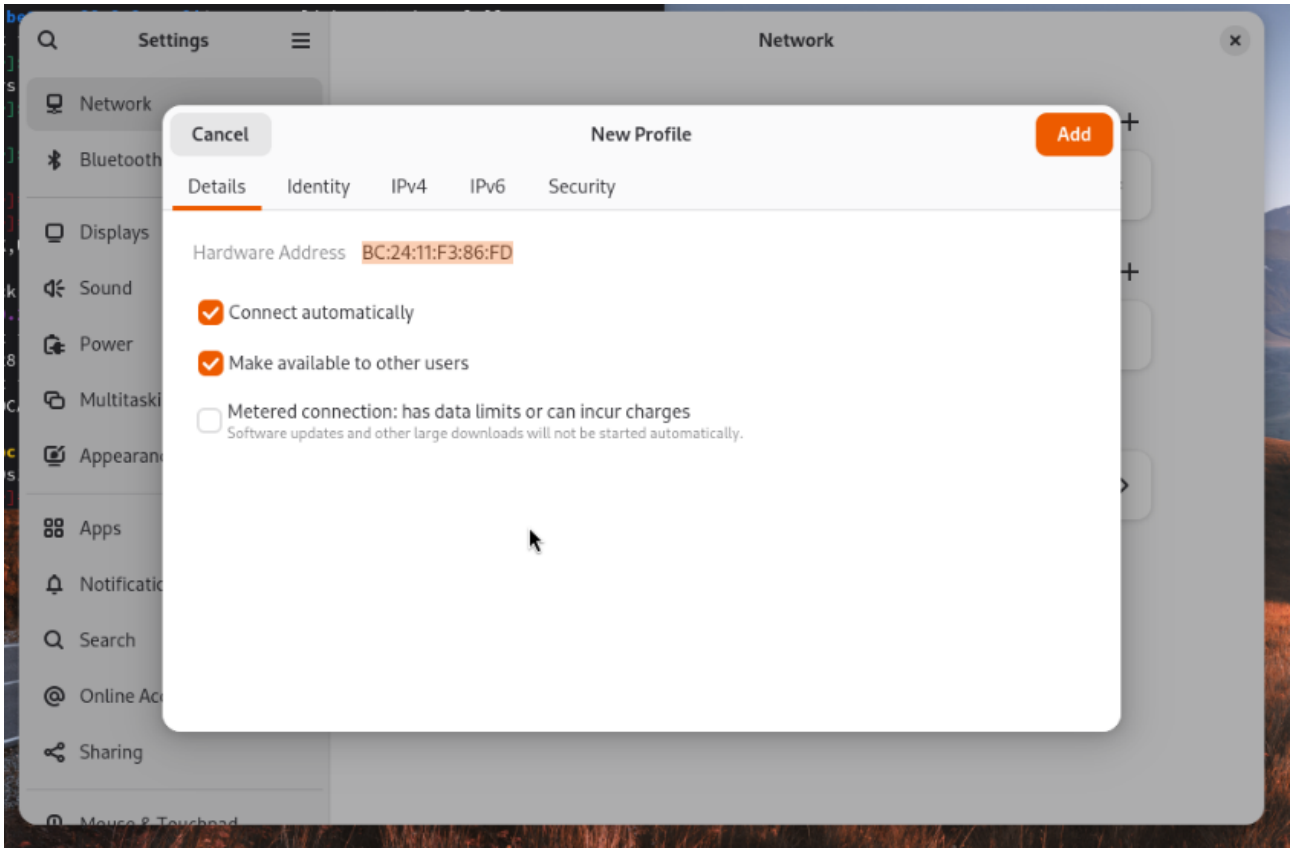
```
[root@sw-cod ~]# passwd net_admin
passwd: updating all authentication tokens for user net_admin.
```

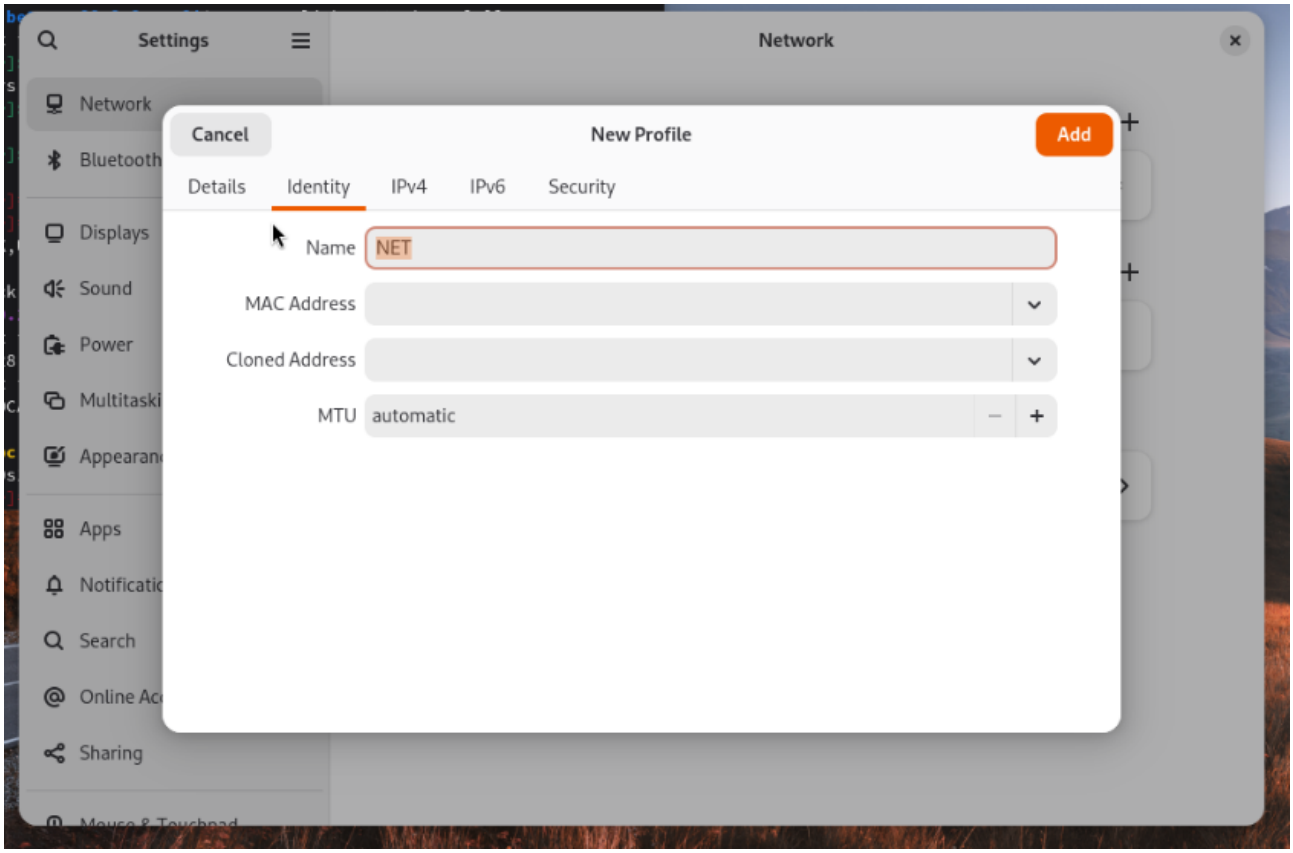
Пробуем зайти под net_admin

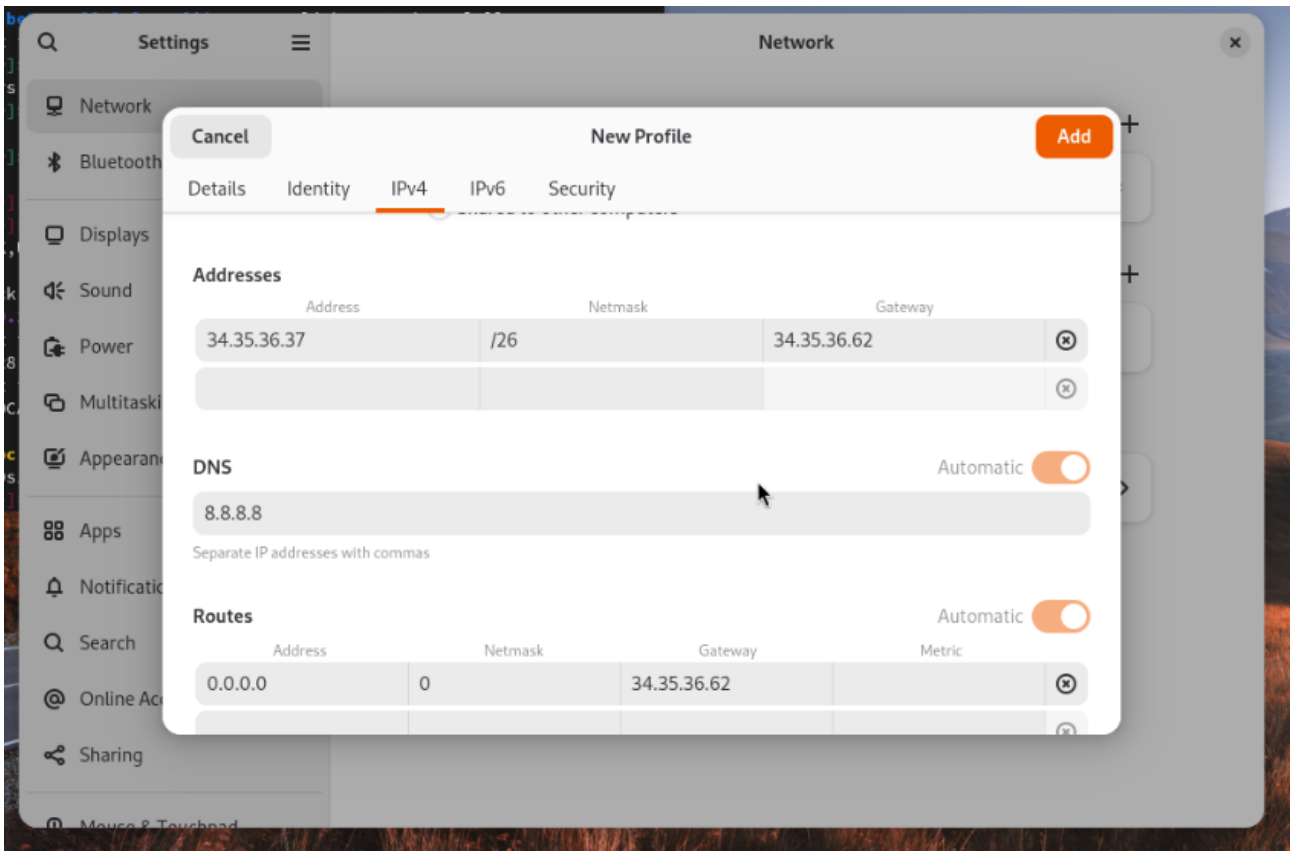
```
Welcome to ALT Server 11.0 (Mendelevium)!

Hostname: sw-cod.au.team
IP: 172.16.1.2
sw-cod login: net_admin
Password:
[net_admin@sw-cod ~]$ sudo su
[root@sw-cod net_admin]# whoami
root
[root@sw-cod net_admin]# exit
exit
[net_admin@sw-cod ~]$ whoami
net_admin
[net_admin@sw-cod ~]$
```

Оба пункта (пароль и рут права) выполнены

----Настройка сети на OUT-CLI----

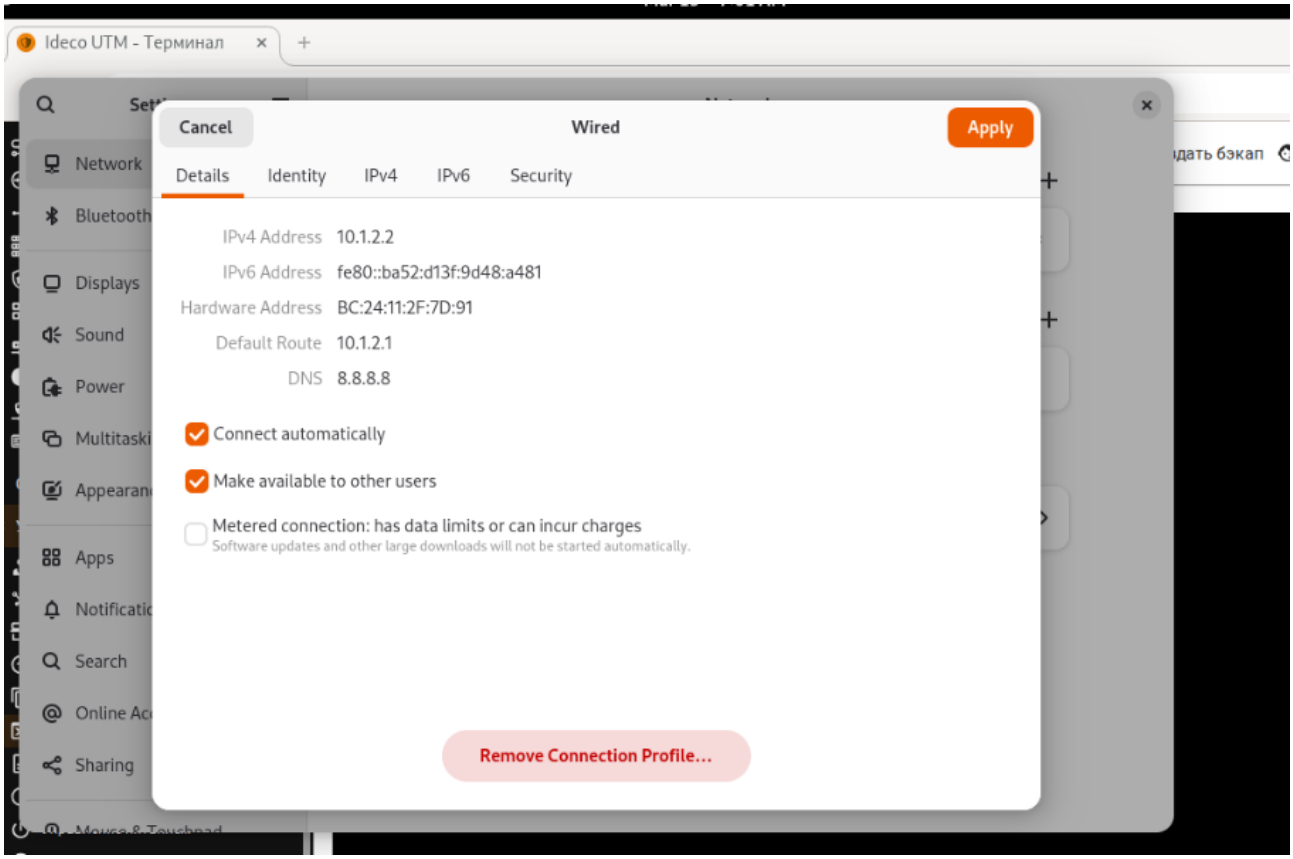




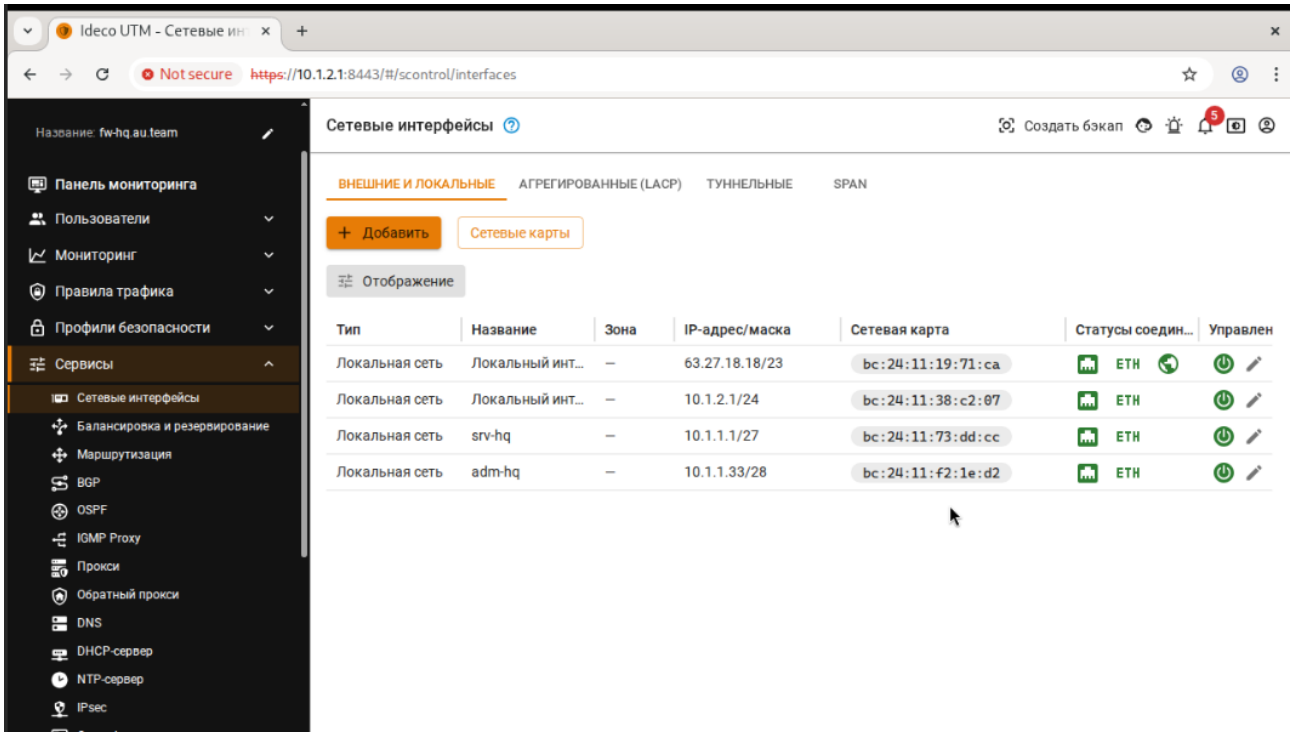

Settings
Network
Bluetooth
Displays
Sound
Power
Multitaski
Appearanc
Apps
Notificatic
Search
Online Ac
Sharing
Network
Cancel
New Profile
Add
Details
Identity
IPv4
IPv6
Security
Addresses
Address
Netmask
Gateway
34.35.36.37
/26
34.35.36.62
DNS
Automatic
8.8.8.8
Separate IP addresses with commas
Routes
Automatic
Address
Netmask
Gateway
Metric
0.0.0.0
0
34.35.36.62

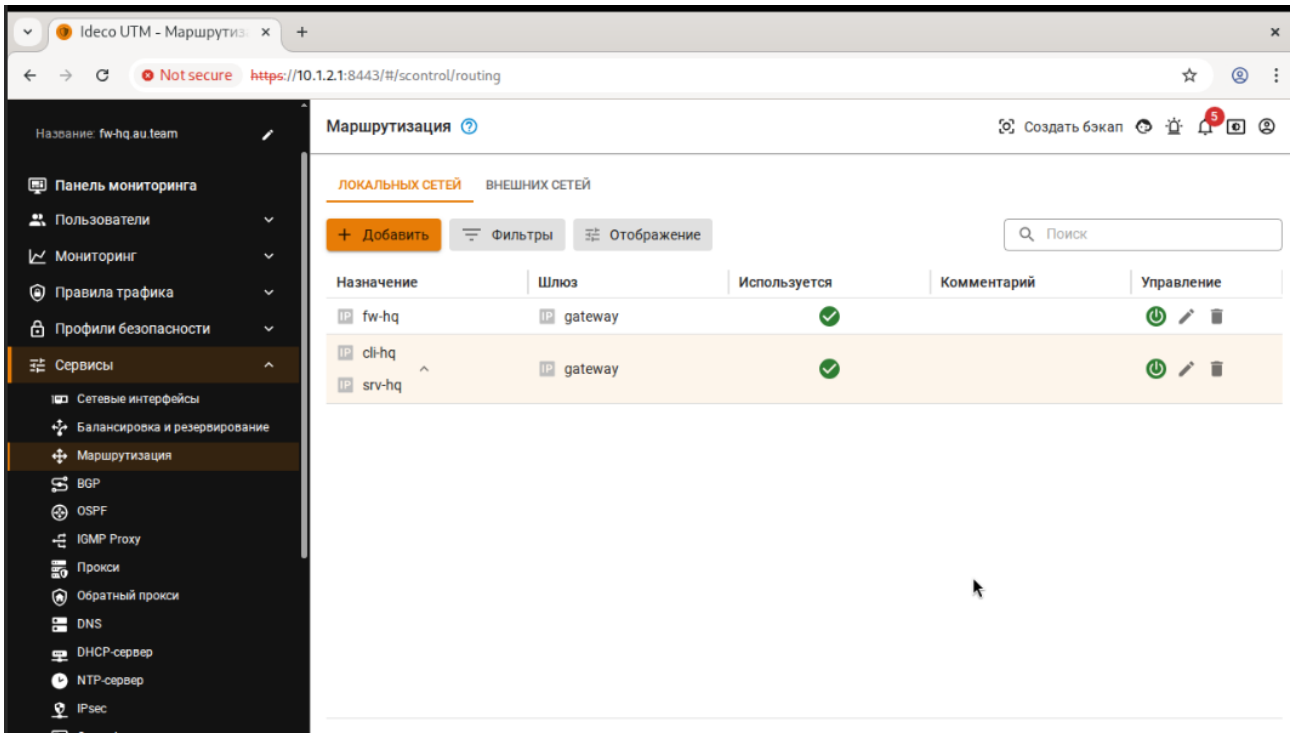
----ADM-HQ----

Настройка доступа к FW-HQ

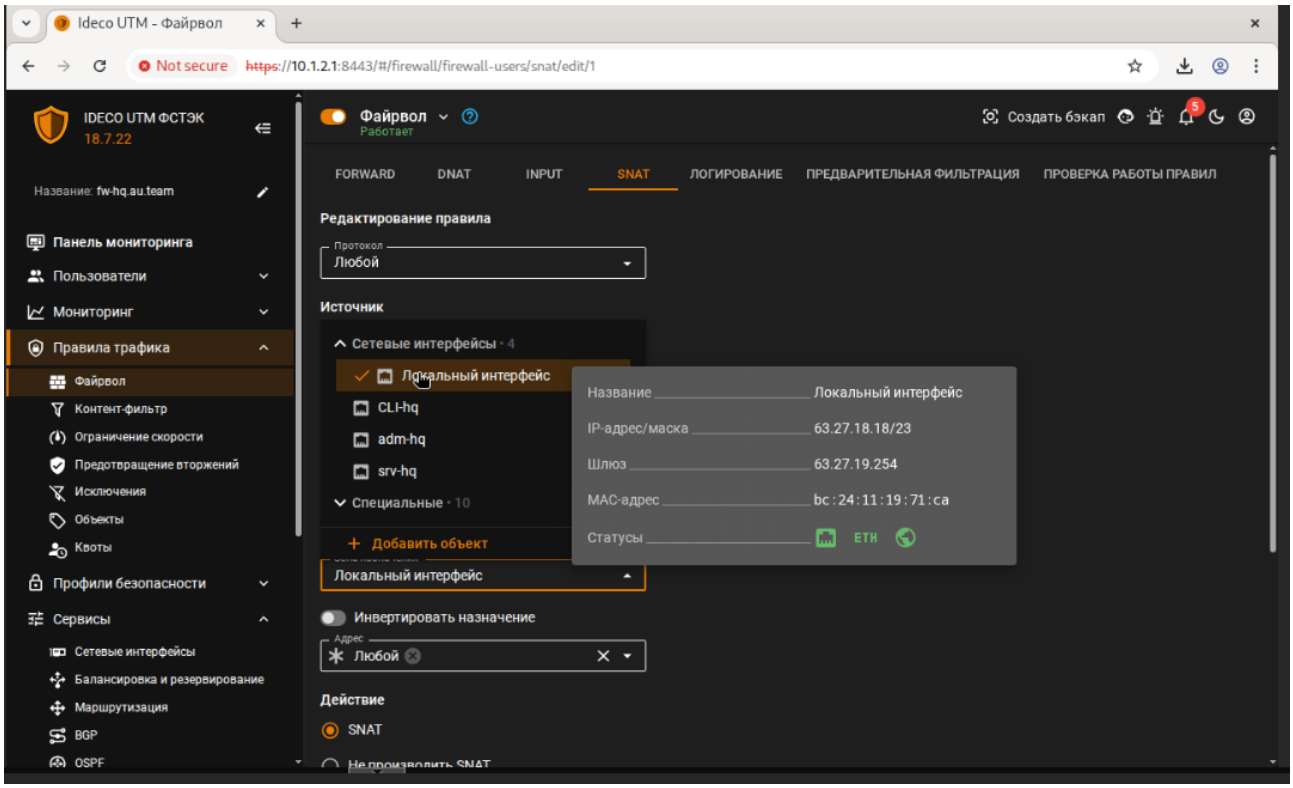


----FW-HQ----



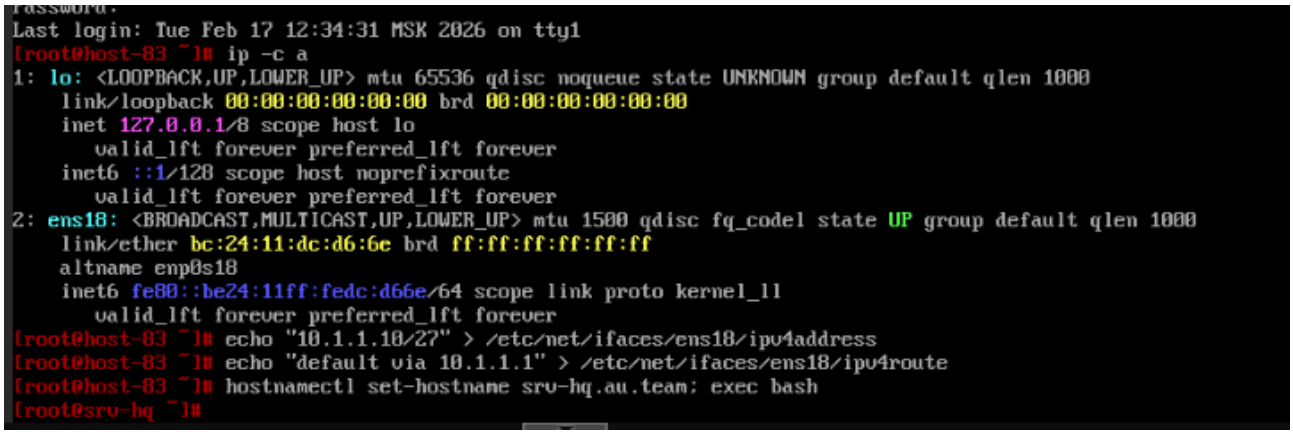


Для доступа в интернет



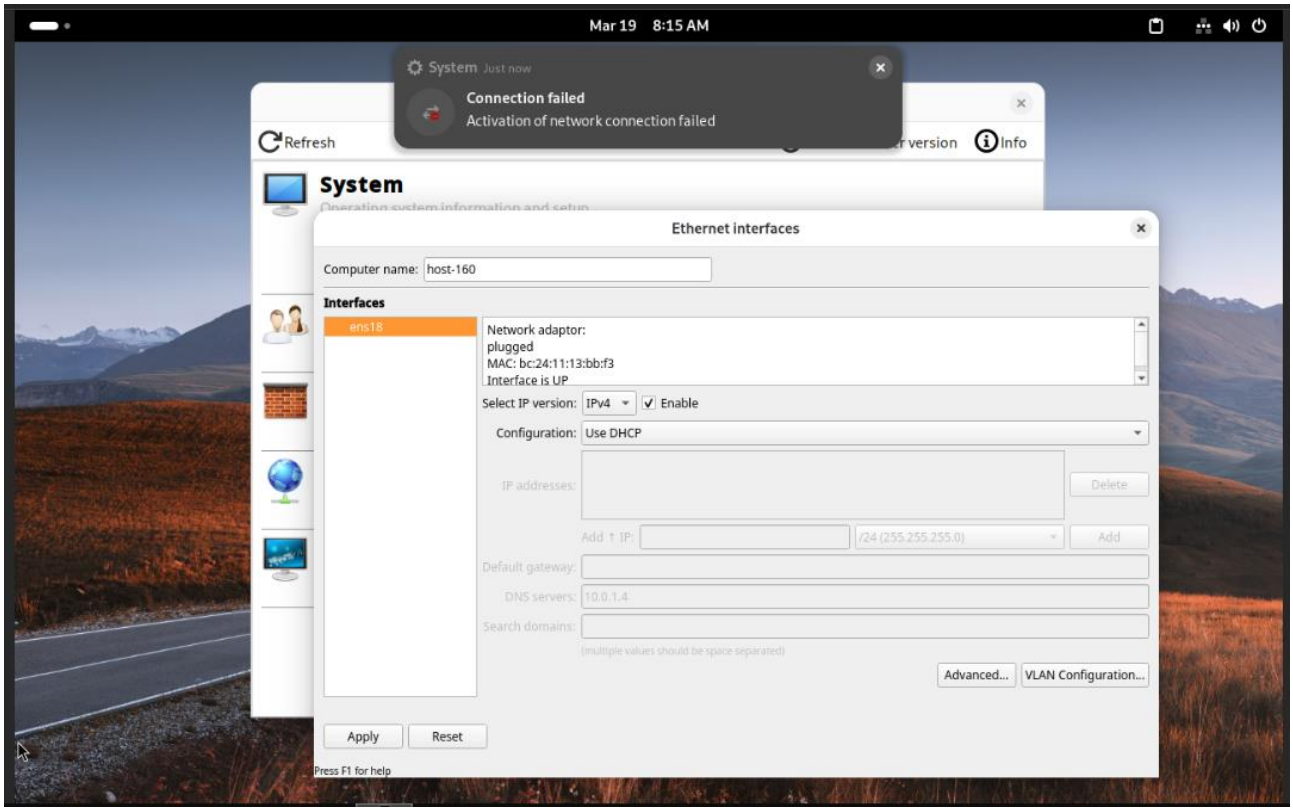
----SRV-HQ----

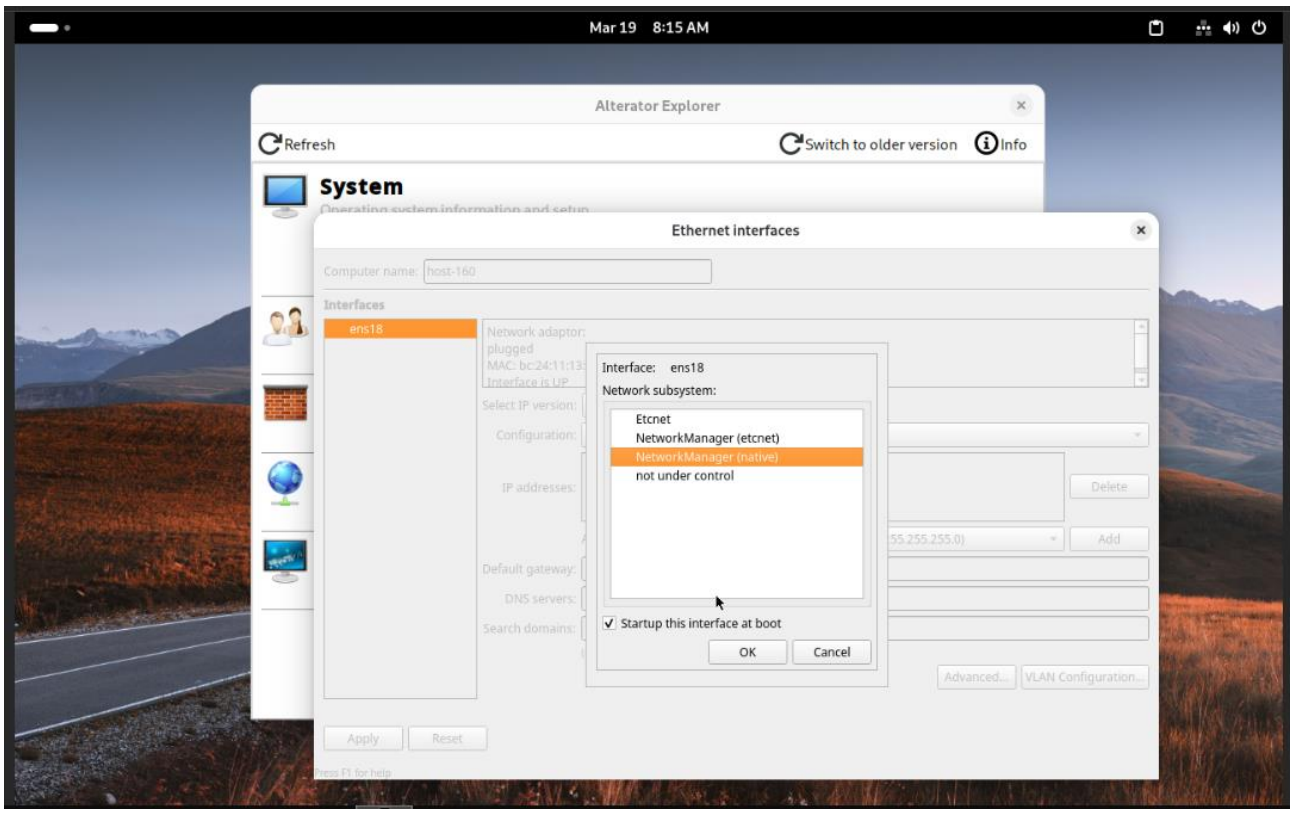
Настройка сети

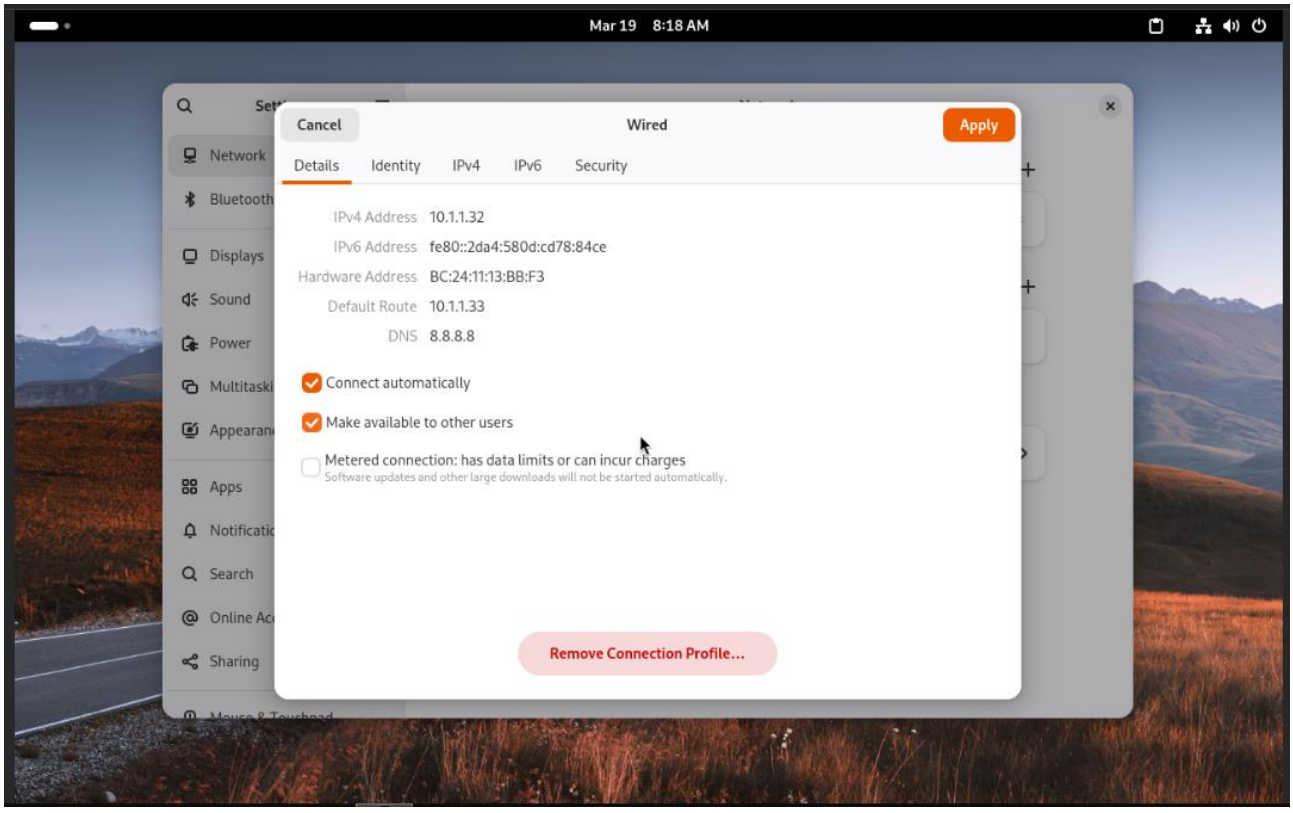


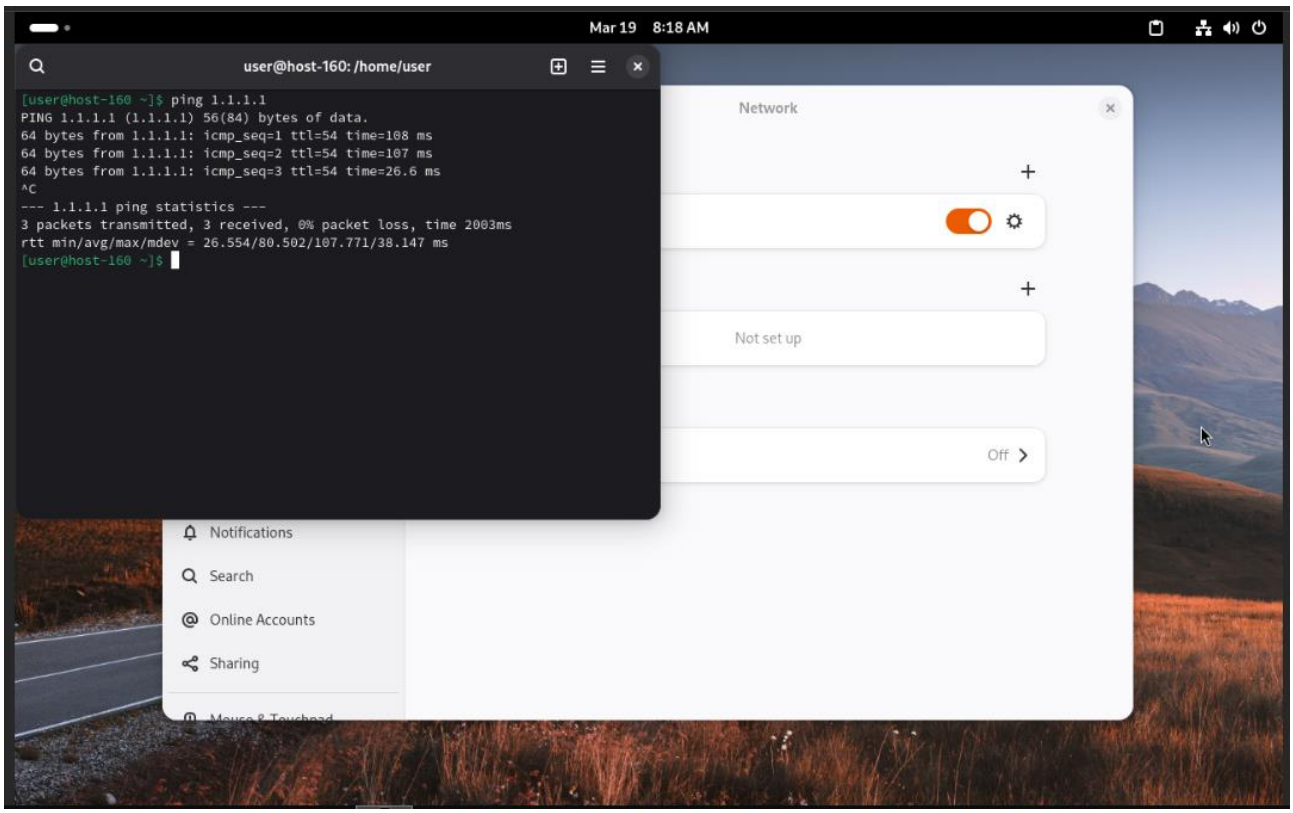
```
[root@srv-hq ~]# systemctl restart network
[root@srv-hq ~]# ip -c a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host proto kernel_lo
       valid_lft forever preferred_lft forever
2: ens18: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether bc:24:11:dc:d6:6e brd ff:ff:ff:ff:ff:ff
    altname enp0s18
    inet 10.1.1.10/27 brd 10.1.1.31 scope global ens18
       valid_lft forever preferred_lft forever
    inet6 fe80::be24:11ff:fedc:d66e/64 scope link proto kernel_ll
       valid_lft forever preferred_lft forever
[root@srv-hq ~]# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=105 time=39.6 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=105 time=39.5 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=105 time=39.4 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=105 time=39.3 ms
^C
--- 8.8.8.8 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 39.320/39.446/39.604/0.116 ms
[root@srv-hq ~]#
```

----CLI-HQ----

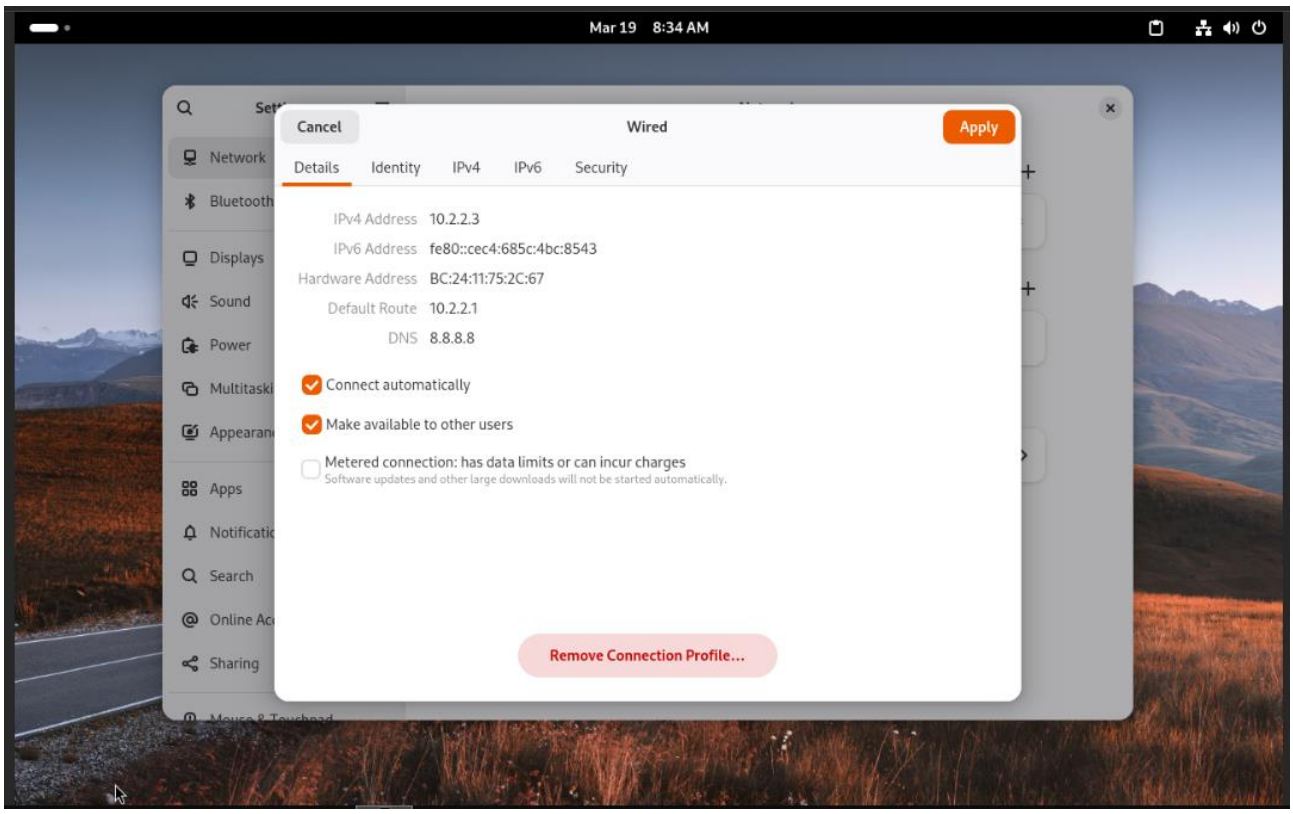


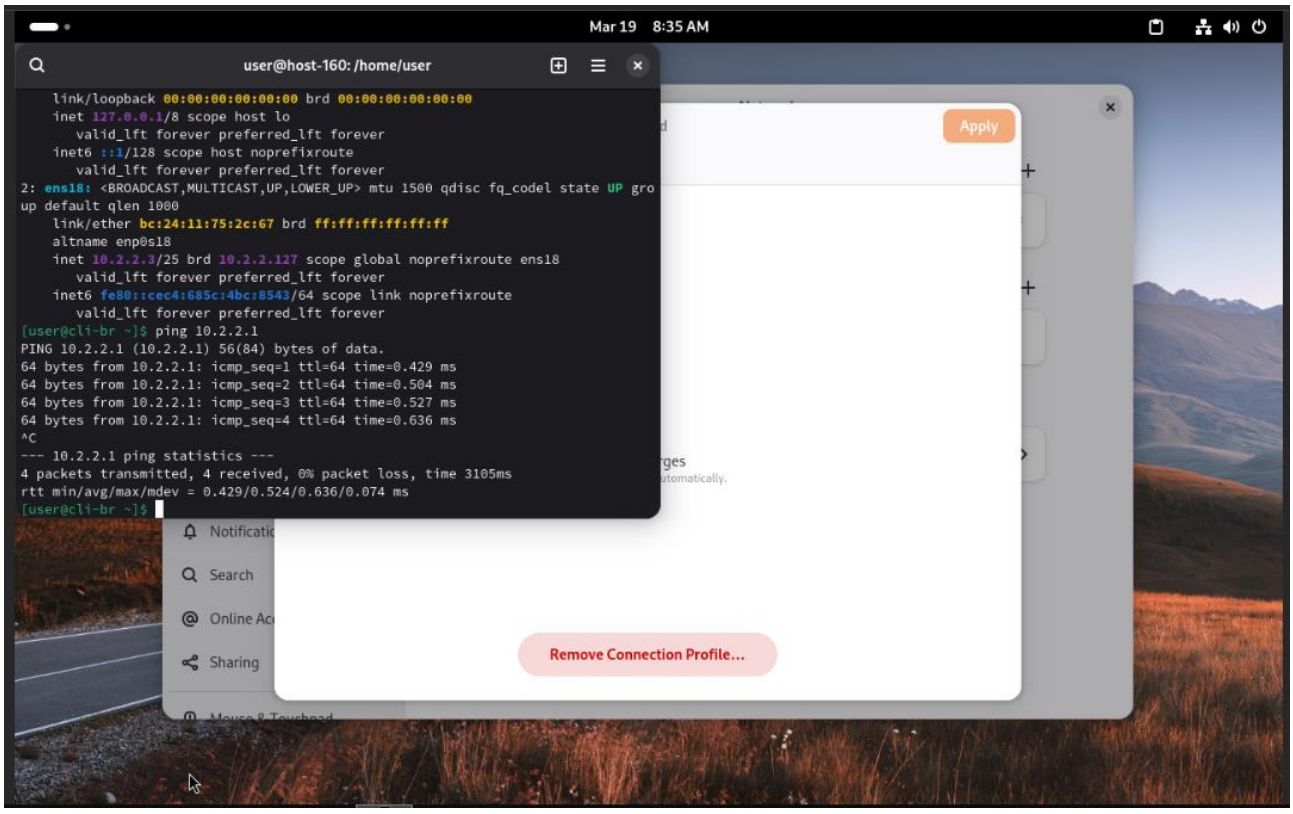

Mar 19 8:15 AM
Alterator Explorer
Refresh
Switch to older version
Info
System
Ethernet interfaces
Computer name: host-160
Interfaces
ens18
Interface: ens18
Network subsystem:
Etcnet
NetworkManager (etcnet)
NetworkManager (native)
not under control
Startup this interface at boot
OK
Cancel
Apply
Reset


Mar 19 8:18 AM
Cancel
Wired
Apply
Details
Identity
IPv4
IPv6
Security
IPv4 Address 10.1.1.32
IPv6 Address fe80::2da4:580d:cd78:84ce
Hardware Address BC:24:11:13:BB:F3
Default Route 10.1.1.33
DNS 8.8.8.8
Connect automatically
Make available to other users
Metered connection: has data limits or can incur charges
Software updates and other large downloads will not be started automatically.
Remove Connection Profile...
Network
Bluetooth
Displays
Sound
Power
Apps
Search
Sharing

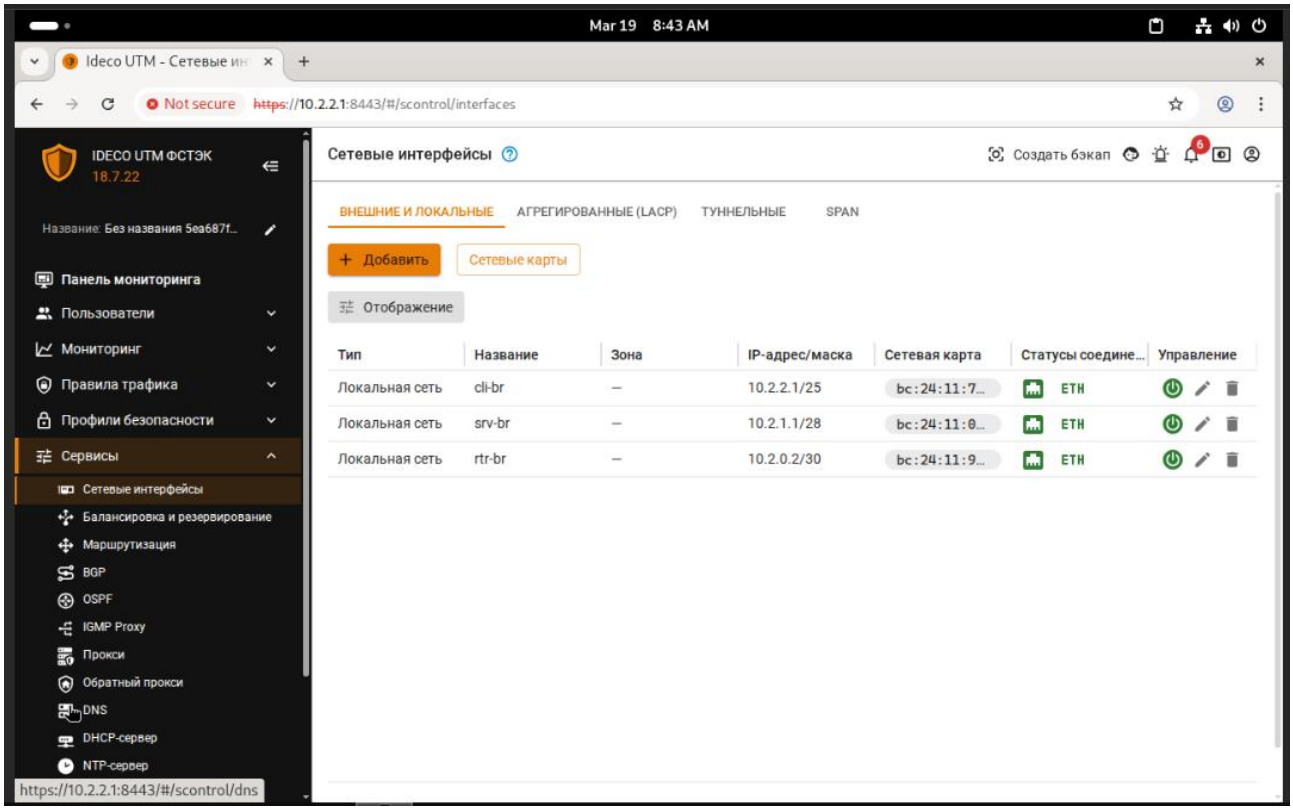

Mar 19 8:18 AM
user@host-160: /home/user
[user@host-160 ~]$ ping 1.1.1.1
PING 1.1.1.1 (1.1.1.1) 56(84) bytes of data.
64 bytes from 1.1.1.1: icmp_seq=1 ttl=54 time=108 ms
64 bytes from 1.1.1.1: icmp_seq=2 ttl=54 time=107 ms
64 bytes from 1.1.1.1: icmp_seq=3 ttl=54 time=26.6 ms
^C
--- 1.1.1.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 26.554/80.502/107.771/38.147 ms
[user@host-160 ~]$
Network
Not set up
Off
Notifications
Search
Online Accounts
Sharing

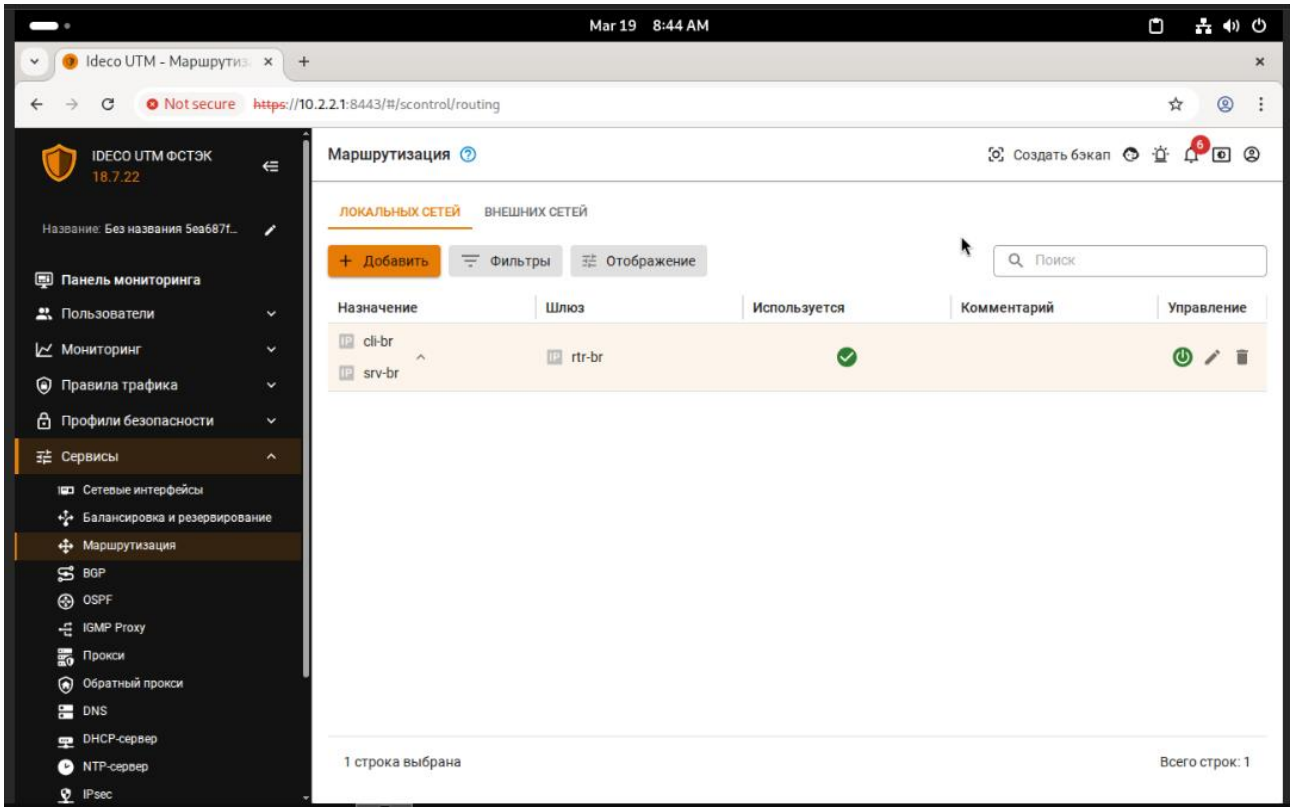
----CLI-BR----


Mar 19 8:34 AM
Cancel
Wired
Apply
Details
Identity
IPv4
IPv6
Security
IPv4 Address 10.2.2.3
IPv6 Address fe80::cec4:685c:4bc:8543
Hardware Address BC:24:11:75:2C:67
Default Route 10.2.2.1
DNS 8.8.8.8
Connect automatically
Make available to other users
Metered connection: has data limits or can incur charges
Software updates and other large downloads will not be started automatically.
Remove Connection Profile...
Network
Bluetooth
Displays
Sound
Power
Apps
Search
Sharing


Mar 19 8:35 AM
user@host-160: /home/user
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
valid_lft forever preferred_lft forever
inet6 ::1/128 scope host noprefixroute
valid_lft forever preferred_lft forever
2: ens18: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP gro
up default qlen 1000
link/ether bc:24:11:75:2c:67 brd ff:ff:ff:ff:ff:ff
altname enp0s18
inet 10.2.2.3/25 brd 10.2.2.127 scope global noprefixroute ens18
valid_lft forever preferred_lft forever
inet6 fe80::cec4:685c:4bc:8543/64 scope link noprefixroute
valid_lft forever preferred_lft forever
[user@cli-br ~]$ ping 10.2.2.1
PING 10.2.2.1 (10.2.2.1) 56(84) bytes of data.
64 bytes from 10.2.2.1: icmp_seq=1 ttl=64 time=0.429 ms
64 bytes from 10.2.2.1: icmp_seq=2 ttl=64 time=0.504 ms
64 bytes from 10.2.2.1: icmp_seq=3 ttl=64 time=0.527 ms
64 bytes from 10.2.2.1: icmp_seq=4 ttl=64 time=0.636 ms
^C
--- 10.2.2.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3105ms
rtt min/avg/max/mdev = 0.429/0.524/0.636/0.074 ms
[user@cli-br ~]$
Apply
Remove Connection Profile...
Search
Sharing

----FW-BR----


Mar 19 8:43 AM
Ideco UTM - Сетевые ин
Not secure https://10.2.2.1:8443/#/scontrol/interfaces
IDECO UTM ФСТЭК
18.7.22
Название: Без названия 5ea687f...
Панель мониторинга
Пользователи
Мониторинг
Правила трафика
Профили безопасности
Сервисы
Сетевые интерфейсы
Балансировка и резервирование
Маршрутизация
BGP
OSPF
IGMP Proxy
Прокси
Обратный прокси
DNS
DHCP-сервер
NTP-сервер
https://10.2.2.1:8443/#/scontrol/dns
Сетевые интерфейсы
Создать бэкап
ВНЕШНИЕ И ЛОКАЛЬНЫЕ
АГРЕГИРОВАННЫЕ (LACP)
ТУННЕЛЬНЫЕ
SPAN
Добавить
Сетевые карты
Отображение
Тип
Название
Зона
IP-адрес/маска
Сетевая карта
Статусы соедине...
Управление
Локальная сеть
cli-br
–
10.2.2.1/25
bc:24:11:7...
ETH
Локальная сеть
srv-br
–
10.2.1.1/28
bc:24:11:0...
ETH
Локальная сеть
rtr-br
–
10.2.0.2/30
bc:24:11:9...
ETH


Mar 19 8:44 AM
Ideco UTM - Маршрутиз
Not secure https://10.2.2.1:8443/#/scontrol/routing
IDECO UTM ФСТЭК
18.7.22
Название: Без названия 5ea687f...
Панель мониторинга
Пользователи
Мониторинг
Правила трафика
Профили безопасности
Сервисы
Сетевые интерфейсы
Балансировка и резервирование
Маршрутизация
BGP
OSPF
IGMP Proxy
Прокси
Обратный прокси
DNS
DHCP-сервер
NTP-сервер
IPsec
Маршрутизация
Создать бэкап
ЛОКАЛЬНЫХ СЕТЕЙ
ВНЕШНИХ СЕТЕЙ
Добавить
Фильтры
Отображение
Поиск
Назначение
Шлюз
Используется
Комментарий
Управление
cli-br
srv-br
rtr-br
1 строка выбрана
Всего строк: 1

----SRV-BR----

```
Last login: Tue Feb 17 12:34:31 MSK 2026 on tty1
[root@host-83 ~]# ip -c a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: ens18: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether bc:24:11:b4:40:73 brd ff:ff:ff:ff:ff:ff
    altname enp0s18
    inet6 fe80::be24:11ff:feb4:4073/64 scope link proto kernel_ll
       valid_lft forever preferred_lft forever
[root@host-83 ~]# echo "10.2.1.2/28" > /etc/net/ifaces/ens18/ipv4address
[root@host-83 ~]# echo "default via 10.2.1.1" > /etc/net/ifaces/ens18/ipv4route
[root@host-83 ~]# hostnamectl set-hostname srv-br.au.team; exec bash
[root@srv-br ~]#
```

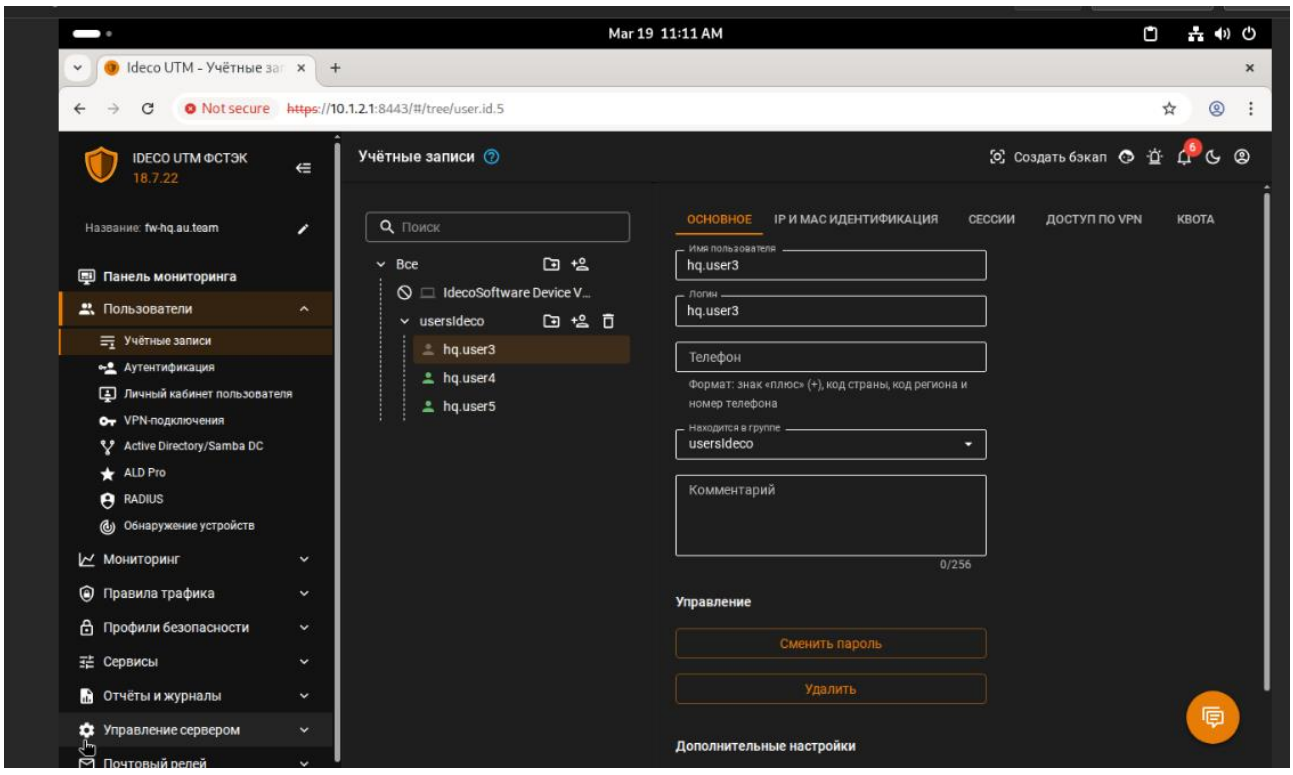
```
 GNU nano 8.0                    /etc/net/ifaces/ens18/options                    Modified
BOOTPROTO=static
TYPE=eth
SYSTEMD_CONTROLLED=no
DISABLED=no
CONFIG_WIRELESS=no
SYSTEMD_BOOTPROTO=static_
CONFIG_IPV4=yes
NM_CONTROLLED=no
```

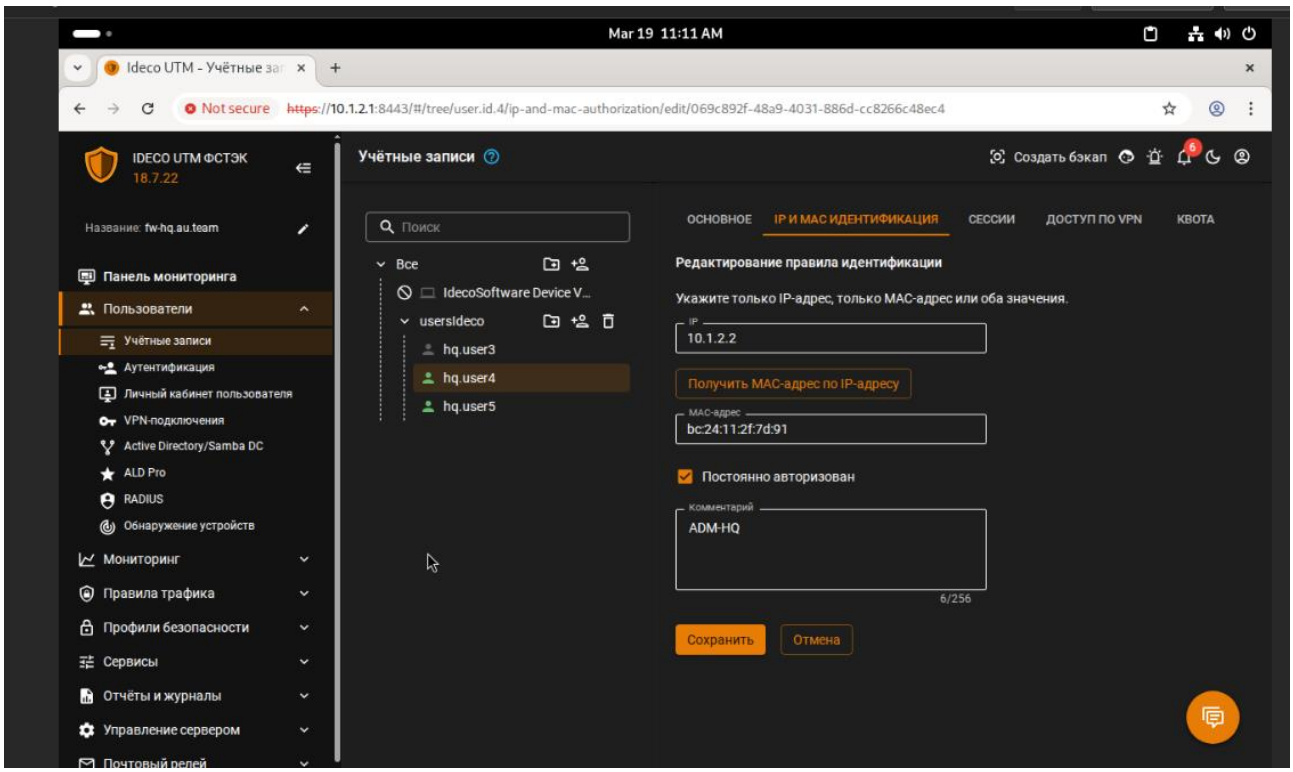
----FW-

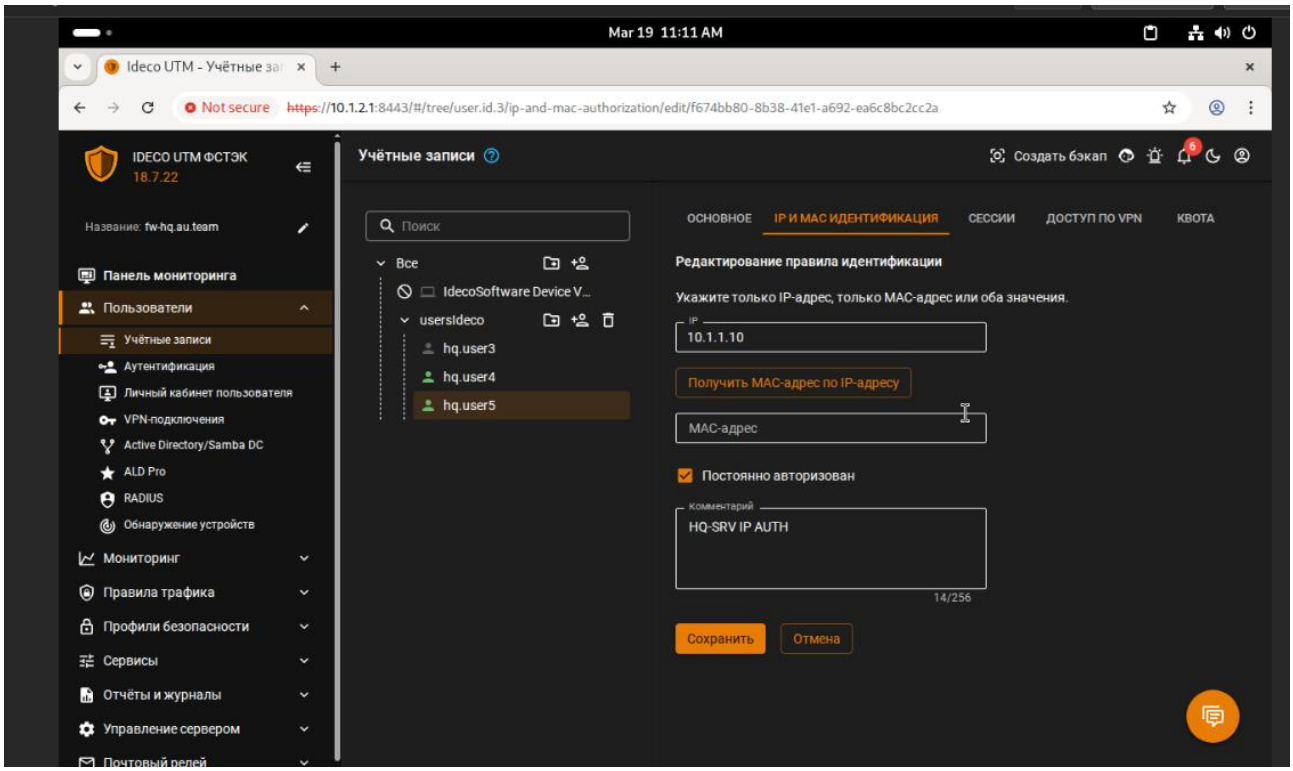
```
[root@srv-br ~]# systemctl restart network
[root@srv-br ~]# ping 1.1.1.1
PING 1.1.1.1 (1.1.1.1) 56(84) bytes of data.
64 bytes from 1.1.1.1: icmp_seq=1 ttl=50 time=52.3 ms
64 bytes from 1.1.1.1: icmp_seq=2 ttl=50 time=47.3 ms
64 bytes from 1.1.1.1: icmp_seq=3 ttl=50 time=46.9 ms
64 bytes from 1.1.1.1: icmp_seq=4 ttl=50 time=47.4 ms
64 bytes from 1.1.1.1: icmp_seq=5 ttl=50 time=47.6 ms
```

HQ----

Создание пользователей и настройка авторизации



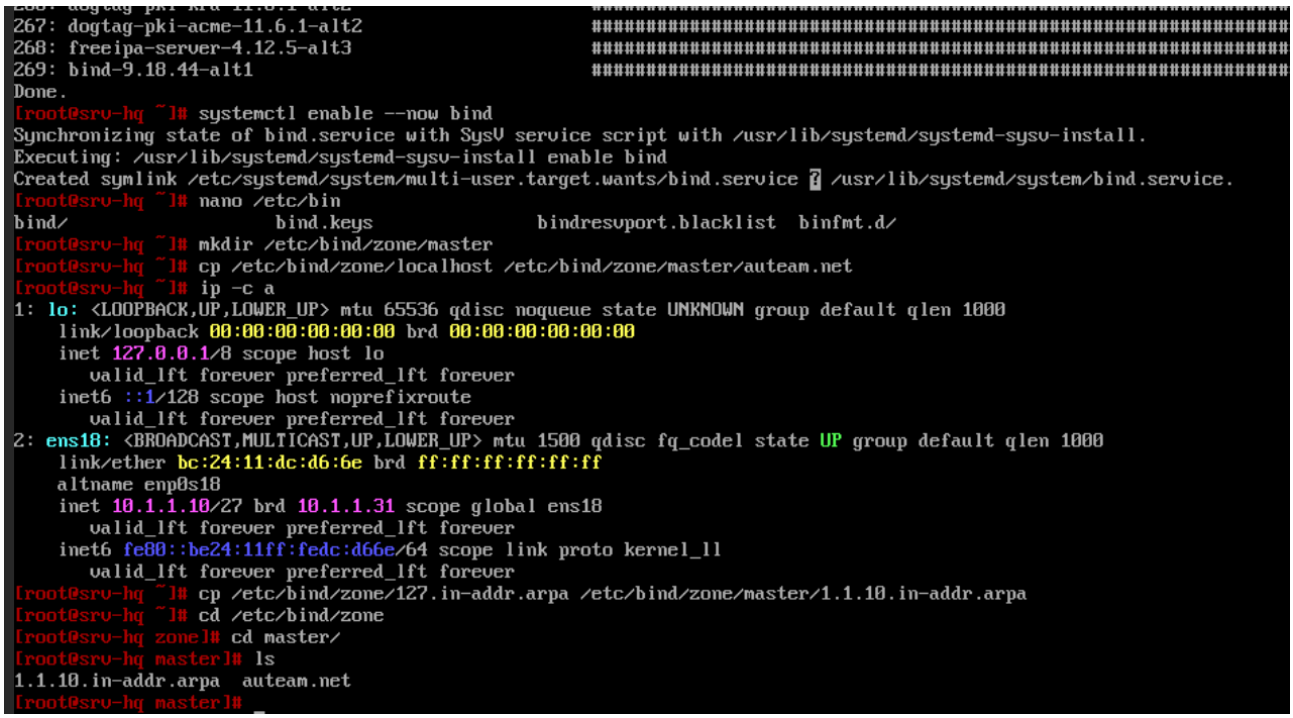

Mar 19 11:11 AM
Ideco UTM - Учётные за
Not secure https://10.1.2.1:8443/#/tree/user.id.4/ip-and-mac-authorization/edit/069c892f-48a9-4031-886d-cc8266c48ec4
IDECO UTM ФСТЭК
18.7.22
Название: fw-hq.au.team
Панель мониторинга
Пользователи
Учётные записи
Аутентификация
Личный кабинет пользователя
VPN-подключения
Active Directory/Samba DC
ALD Pro
RADIUS
Обнаружение устройств
Мониторинг
Правила трафика
Профили безопасности
Сервисы
Отчёты и журналы
Управление сервером
Почтовый релей
Учётные записи
Создать бэкап
Поиск
Все
IdecoSoftware Device V...
usersIdeco
hq.user3
hq.user4
hq.user5
ОСНОВНОЕ
IP И MAC ИДЕНТИФИКАЦИЯ
СЕССИИ
ДОСТУП ПО VPN
КВОТА
Редактирование правила идентификации
Укажите только IP-адрес, только MAC-адрес или оба значения.
IP
10.1.2.2
Получить MAC-адрес по IP-адресу
MAC-адрес
bc:24:11:2f:7d:91
Постоянно авторизован
Комментарий
ADM-HQ
6/256
Сохранить
Отмена


Mar 19 11:11 AM
Ideco UTM - Учётные за
Not secure https://10.1.2.1:8443/#/tree/user.id.3/ip-and-mac-authorization/edit/f674bb80-8b38-41e1-a692-ea6c8bc2cc2a
IDECO UTM ФСТЭК
18.7.22
Название: fw-hq.au.team
Панель мониторинга
Пользователи
Учётные записи
Аутентификация
Личный кабинет пользователя
VPN-подключения
Active Directory/Samba DC
ALD Pro
RADIUS
Обнаружение устройств
Мониторинг
Правила трафика
Профили безопасности
Сервисы
Отчёты и журналы
Управление сервером
Почтовый релей
Учётные записи
Создать бэкап
Поиск
Все
IdecoSoftware Device V...
usersIdeco
hq.user3
hq.user4
hq.user5
ОСНОВНОЕ
IP И MAC ИДЕНТИФИКАЦИЯ
СЕССИИ
ДОСТУП ПО VPN
КВОТА
Редактирование правила идентификации
Укажите только IP-адрес, только MAC-адрес или оба значения.
IP
10.1.1.10
Получить MAC-адрес по IP-адресу
MAC-адрес
Постоянно авторизован
Комментарий
HQ-SRV IP AUTH
14/256
Сохранить
Отмена

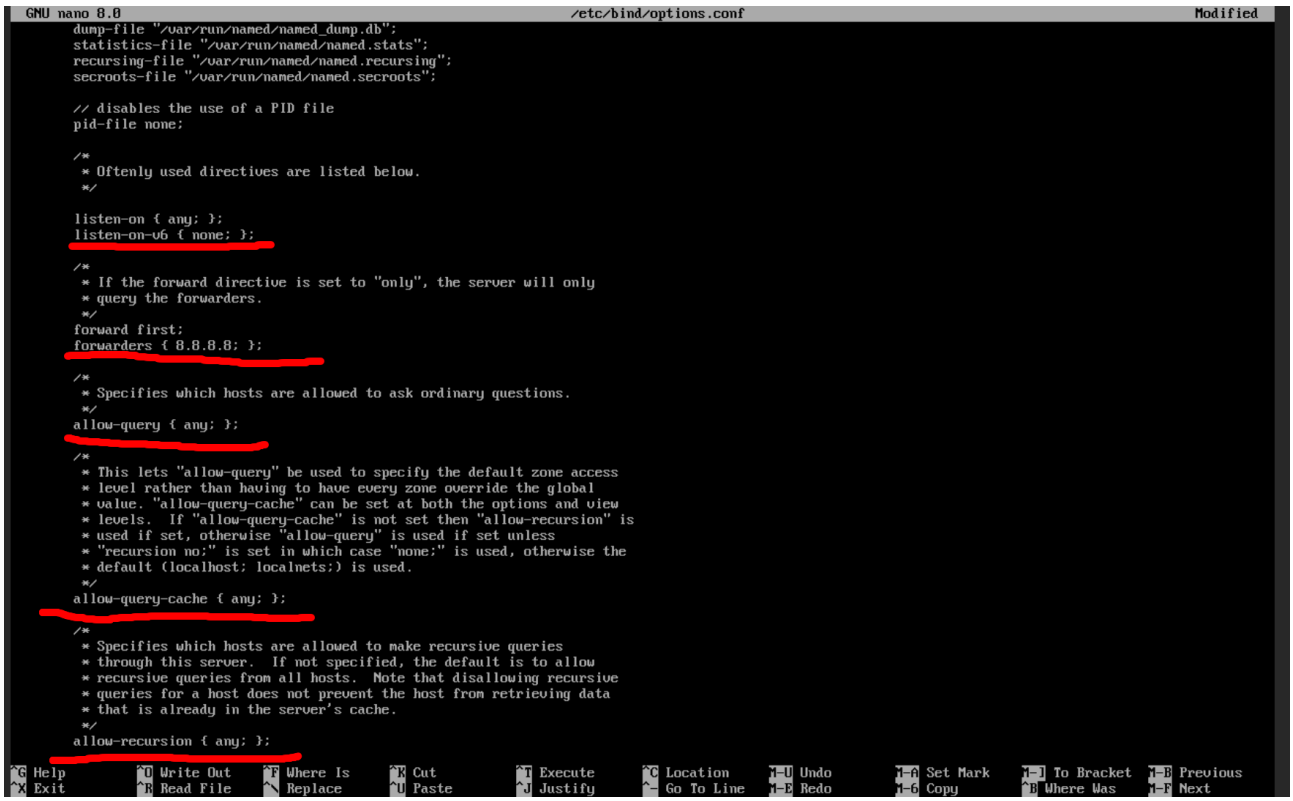
----SRV-HQ----

----BIND9 НАСТРОЙКА DNS СЕРВЕРА----

```
[root@srv-hq master]# apt-get install freeipa-server freeipa-dns bind bind-utils -y
```



Правим файл /etc/bind/options.conf



Редактируем файл /etc/bind/rfc1912.conf

```
[root@srv-hq zone]# cat /etc/bind/rfc1912.conf
// Be authoritative for the localhost forward and reverse zones,
// and for broadcast zones as per RFC 1912.

zone "localhost" {
        type master;
        file "localhost";
        allow-update { none; };
};

zone "localdomain" {
        type master;
        file "localdomain";
        allow-update { none; };
};

zone "127.in-addr.arpa" {
        type master;
        file "127.in-addr.arpa";
        allow-update { none; };
};

zone "0.in-addr.arpa" {
        type master;
        file "empty";
        allow-update { none; };
};

zone "255.in-addr.arpa" {
        type master;
        file "empty";
        allow-update { none; };
};

zone "au.team" {
        type master;
        file "au.team";
        allow-transfer { 10.1.1.10; };
};

zone "1.10.in-addr.arpa" {
        type master;
        file "1.10.in-addr.arpa";
        allow-transfer { 10.1.1.10; };
};
[root@srv-hq zone]#
```

Правим файл /etc/bind/zone/au.team

```
[root@srv-hq zone]# cat au.team
$TTL    1D
@               IN      SOA             au.team.        root.au.team. (
                                        2026012400      ; serial
                                        12H             ; refresh
                                        1H              ; retry
                                        1W              ; expire
                                        1H              ; ncache
                                )
@               IN      NS      srv-hq.au.team.
srv-hq          IN      A       10.1.1.10
fw-hq           IN      A       10.1.1.1
adm-hq          IN      A       10.1.2.2
cli-hq          IN      A       10.1.1.32
monitoring      IN      CNAME   srv-hq.au.team.
[root@srv-hq zone]#
```

Файл /etc/bind/zone/1.10.in-addr.arpa

```
monitoring      IN      CNAME   srv-hq.au.team.
[root@srv-hq zone]# cat 1.10.in-addr.arpa
$TTL    1D
@       IN      SOA     au.team. root.au.team. (
                                2026012400      ; serial
                                12H             ; refresh
                                1H              ; retry
                                1W              ; expire
                                1H              ; ncache
                        )
@       IN      NS      srv-hq.au.team.
1.1     IN      PTR     fw-hq.au.team.
2.2     IN      PTR     adm-hq.au.team.
10.1    IN      PTR     srv-hq.au.team.
32.1    IN      PTR     cli-hq.au.team.
[root@srv-hq zone]#
```

Выдаем права на зоны

chown root:named /etc/bind/zone/au.team
chown root:named /etc/bind/zone/1.10.in-addr.arpa

Перезапускаем и проверяем DNS сервер

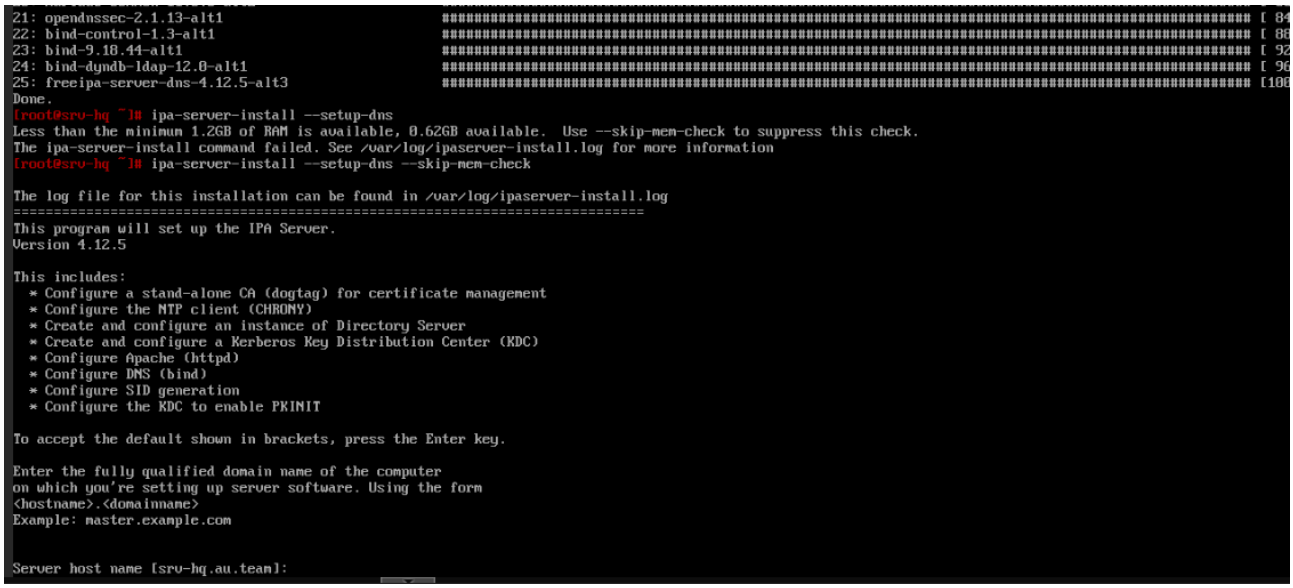
systemctl restart bind

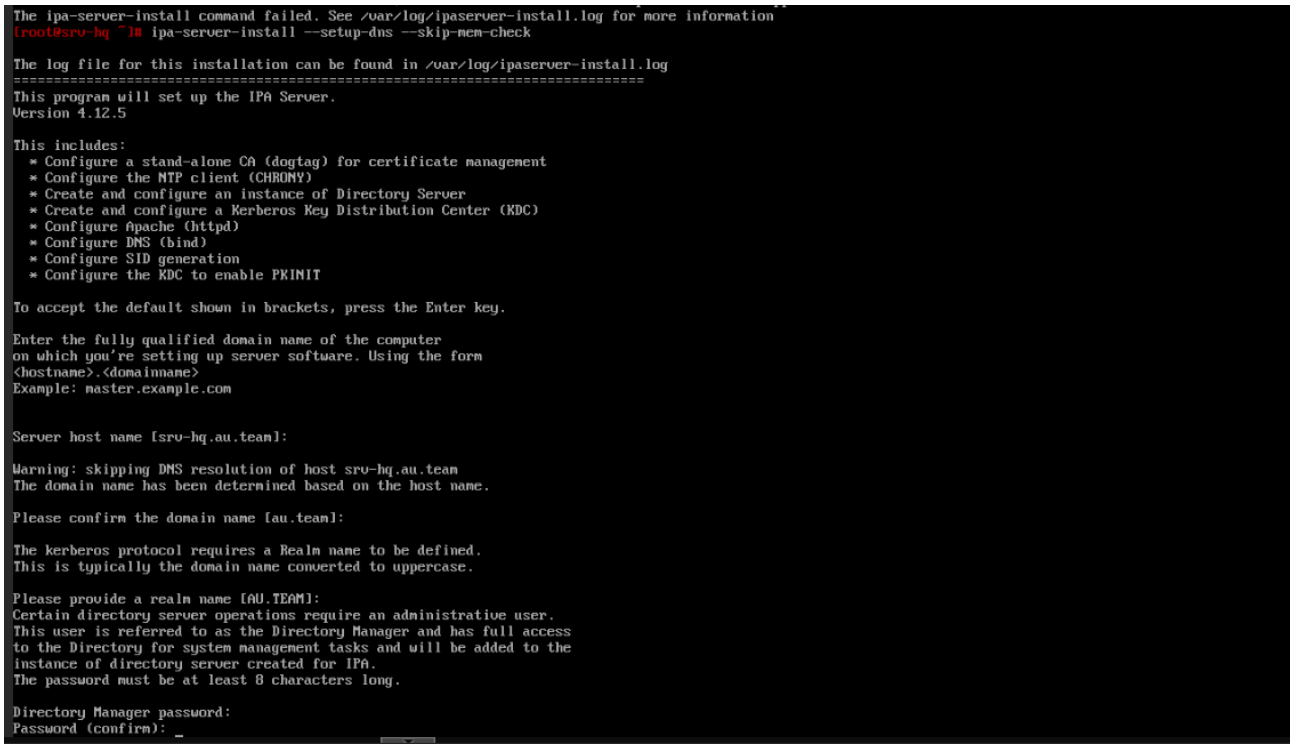
dig @127.0.0.1 fw-hq.au.team

---- установка и настройка FreeIPA ----

Установка FreeIPA

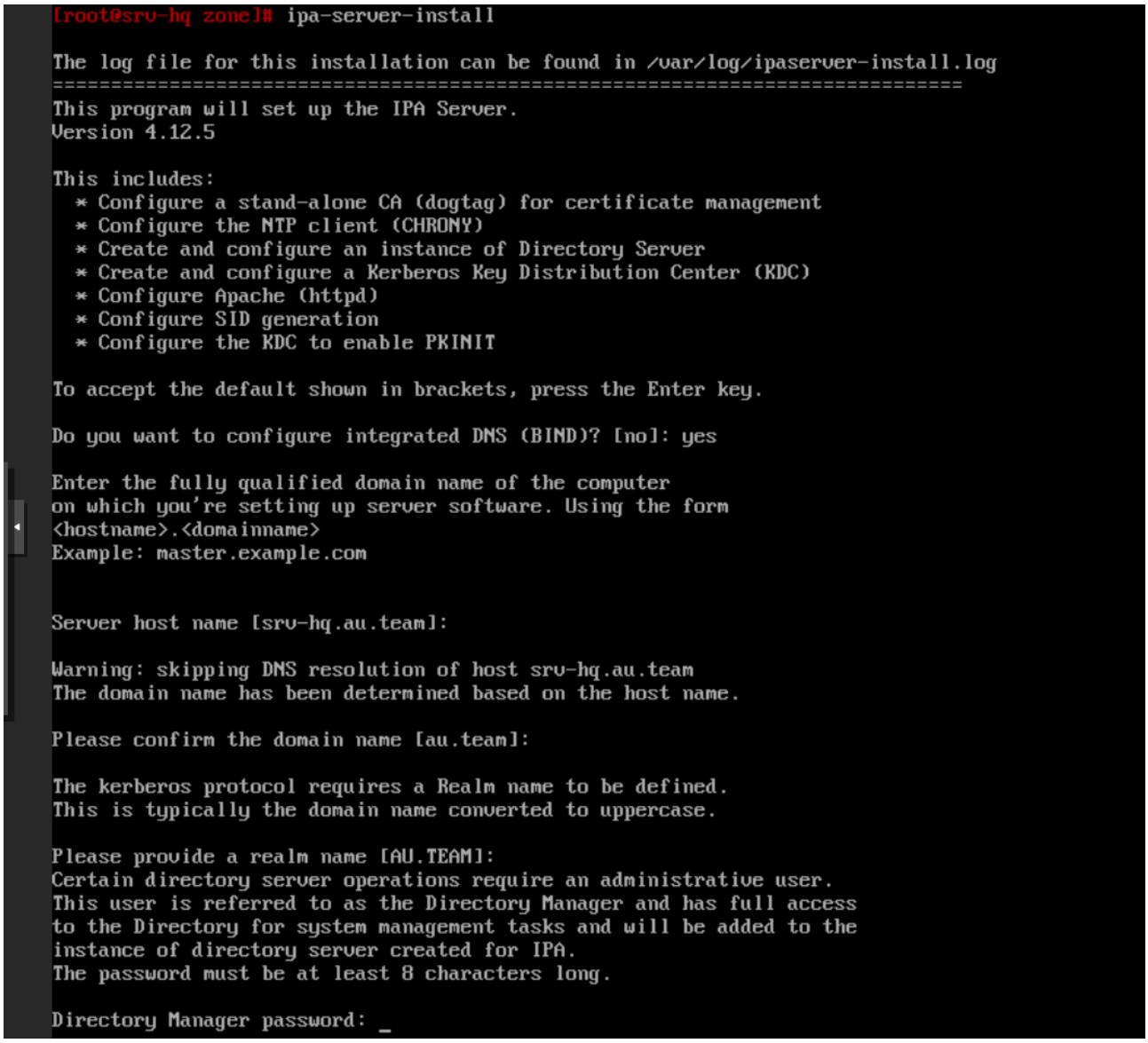
apt-get update && apt-get install chrony freeipa-server freeipa-client freeipa-server-dns -y





Установка

```
ipa-server-install --setup-dns --ssh-trust-dns --mkhomedir --allow-zone-overlap
```



```
Client hostname: srv-hq.au.team
Realm: AU.TEAM
DNS Domain: au.team
IPA Server: srv-hq.au.team
BaseDN: dc=au,dc=team

Configured /etc/sssd/sssd.conf
Systemwide CA database updated.
Adding SSH public key from /etc/openssh/ssh_host_ecdsa_key.pub
Adding SSH public key from /etc/openssh/ssh_host_rsa_key.pub
Adding SSH public key from /etc/openssh/ssh_host_ed25519_key.pub
Configured passwd in /etc/nsswitch.conf
Configured group in /etc/nsswitch.conf
Configured netgroup in /etc/nsswitch.conf
Configured automount in /etc/nsswitch.conf
Configured services in /etc/nsswitch.conf
Configured sudoers in /etc/nsswitch.conf
SSSD enabled
Configured /etc/openldap/ldap.conf
Configured /etc/openssh/ssh_config
Configured /etc/openssh/sshd_config
Configuring au.team as NIS domain.
Client configuration complete.
The ipa-client-install command was successful

Invalid IP address fe80::be24:11ff:fedc:d66e for srv-hq.au.team.: cannot use link-local IP address fe80::be24:11ff:fedc:d66e
==============================================================================
Setup complete

Next steps:
        1. You must make sure these network ports are open:
                TCP Ports:
                  * 80, 443: HTTP/HTTPS
                  * 389, 636: LDAP/LDAPS
                  * 88, 464: kerberos
                  * 53: bind
                UDP Ports:
                  * 88, 464: kerberos
                  * 53: bind
                  * 123: ntp

        2. You can now obtain a kerberos ticket using the command: 'kinit admin'
           This ticket will allow you to use the IPA tools (e.g., ipa user-add)
           and the web user interface.

Be sure to back up the CA certificates stored in /root/cacert.p12
These files are required to create replicas. The password for these
files is the Directory Manager password
The ipa-server-install command was successful
[root@srv-hq ~]#
```

ipa-server-install --setup-dns --ssh-trust-dns --mkhomedir --allow-zone-overlap

```
NetBIOS domain name [AU]:

Do you want to configure CHRONY with NTP server or pool address? [no]:

The IPA Master Server will be configured with:
Hostname:       srv-hq.au.team
IP address(es): 10.1.1.10
Domain name:    au.team
Realm name:     AU.TEAM

The CA will be configured with:
Subject DN:   CN=Certificate Authority,O=AU.TEAM
Subject base: O=AU.TEAM
Chaining:     self-signed

BIND DNS server will be configured to serve IPA domain with:
Forwarders:       127.0.0.1, 8.8.8.8
Forward policy:   only
Reverse zone(s):  No reverse zone

Continue to configure the system with these values? [no]: yes
[Errno 2] No such file or directory: '/var/lib/ipa/sysrestore/sysrestore.state'
The ipa-server-install command failed. See /var/log/ipaserver-install.log for more information
[root@srv-hq zone]#
```

```
[root@srv-hq bind]# cat ipa-options-ext.conf
/* User customization for BIND named
 *
 * This file is included in /etc/bind/named.conf and is not modified during IPA
 * upgrades.
 *
 * It must only contain "options" settings. Any other setting must be
 * configured in /etc/bind/ipa-ext.conf.
 *
 * Examples:
 * allow-recursion { any; };
 * allow-query-cache { any; };
 */

/* turns on IPv6 for port 53, IPv4 is on by default for all ifaces */
listen-on-v6 { any; };
listen-on { any; };

/* dnssec-enable is obsolete and 'yes' by default */
dnssec-validation no;


forward first;
forwarders { 8.8.8.8; };
[root@srv-hq bind]# pwd
/etc/bind
[root@srv-hq bind]#
```

----СОЗДАНИЕ ПОЛЬЗОВАТЕЛЕЙ НА СЕРВЕРЕ FREEIPA----

```
[root@srv-hq ~]# ipa user-add
First name: hq.user1
Last name: hq.user1
User login [hhq.user1]: hq.user1
---------------------
Added user "hq.user1"
---------------------
  User login: hq.user1
  First name: hq.user1
  Last name: hq.user1
  Full name: hq.user1 hq.user1
  Display name: hq.user1 hq.user1
  Initials: hh
  Home directory: /home/hq.user1
  GECOS: hq.user1 hq.user1
  Login shell: /bin/bash
  Principal name: hq.user1@AU.TEAM
  Principal alias: hq.user1@AU.TEAM
  Email address: hq.user1@au.team
  UID: 235400003
  GID: 235400003
  Password: False
  Member of groups: ipausers
  Kerberos keys available: False
[root@srv-hq ~]#
```

Пользователи

X.user1

X.user2

X.user3

X.user4

X.user5

Где X имя зоны (hq, br, cod)

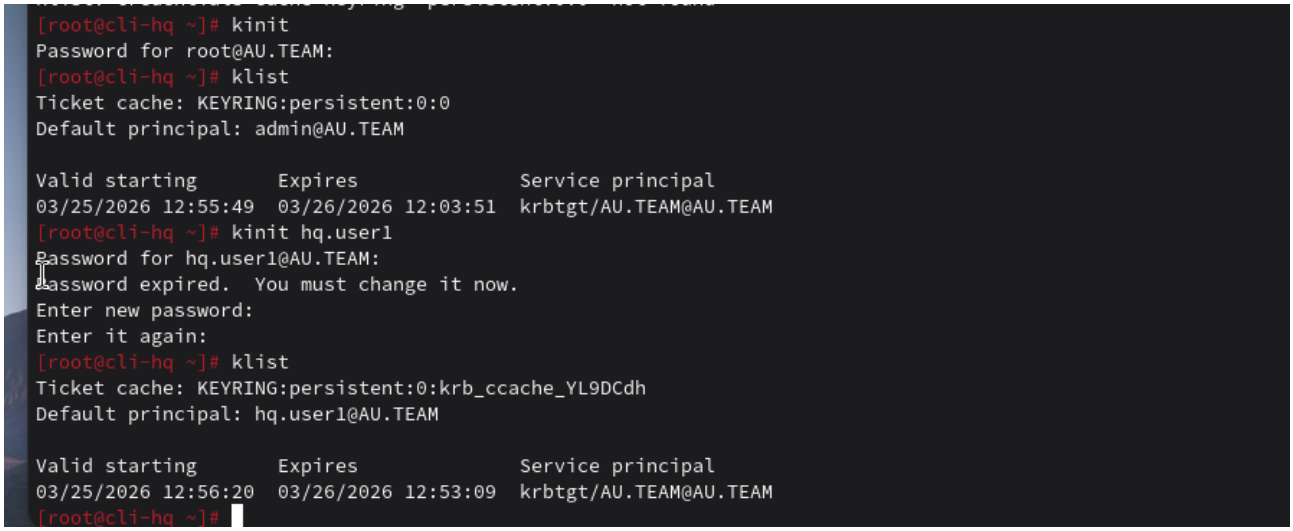
```
  Principal alias: hq.user3@AU.TEAM
  Email address: hq.user3@au.team
  UID: 235400005
  GID: 235400005
  Password: False
  Member of groups: ipausers
  Kerberos keys available: False
[root@srv-hq ~]# ipa user-add --first=hq.user4 --last=hq.user4 hq.user4
----------------------
Added user "hq.user4"
----------------------
  User login: hq.user4
  First name: hq.user4
  Last name: hq.user4
  Full name: hq.user4 hq.user4
  Display name: hq.user4 hq.user4
  Initials: hh
  Home directory: /home/hq.user4
  GECOS: hq.user4 hq.user4
  Login shell: /bin/bash
  Principal name: hq.user4@AU.TEAM
  Principal alias: hq.user4@AU.TEAM
  Email address: hq.user4@au.team
  UID: 235400006
  GID: 235400006
  Password: False
  Member of groups: ipausers
  Kerberos keys available: False
[root@srv-hq ~]# ipa user-add --first=hq.user5 --last=hq.user5 hq.user5
----------------------
Added user "hq.user5"
----------------------
  User login: hq.user5
  First name: hq.user5
  Last name: hq.user5
  Full name: hq.user5 hq.user5
  Display name: hq.user5 hq.user5
  Initials: hh
  Home directory: /home/hq.user5
  GECOS: hq.user5 hq.user5
  Login shell: /bin/bash
  Principal name: hq.user5@AU.TEAM
  Principal alias: hq.user5@AU.TEAM
  Email address: hq.user5@au.team
  UID: 235400007
  GID: 235400007
  Password: False
  Member of groups: ipausers
  Kerberos keys available: False
[root@srv-hq ~]#
```

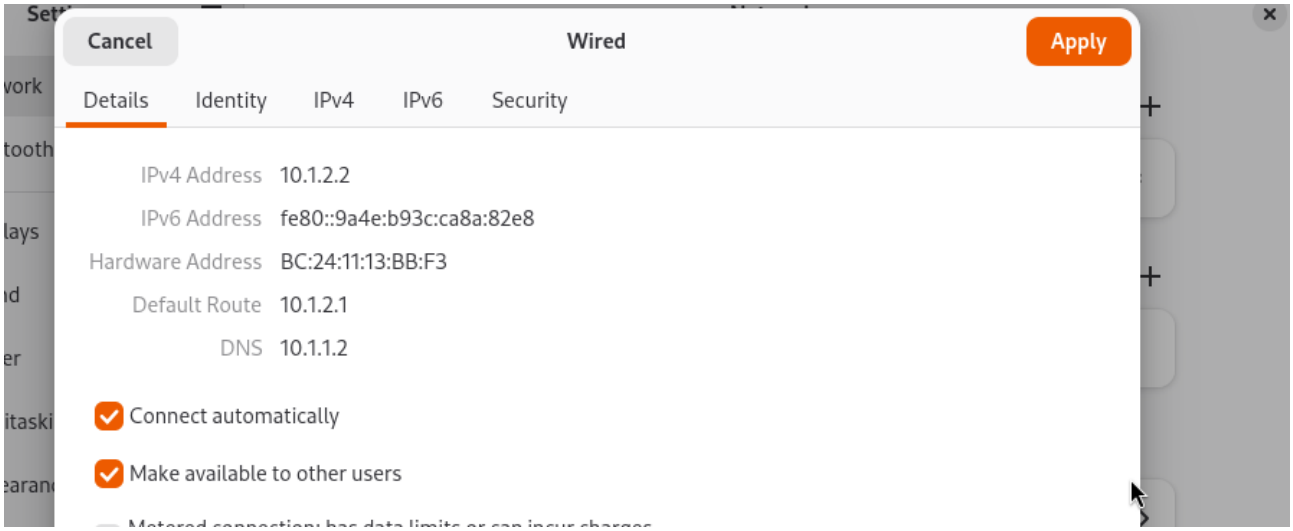
```
  Password: True
  Member of groups: ipausers
  Kerberos keys available: True
[root@srv-hq ~]# ipa user-mod hq.user4 --password
Password:
Enter Password again to verify:
-----------------------
Modified user "hq.user4"
-----------------------
  User login: hq.user4
  First name: hq.user4
  Last name: hq.user4
  Home directory: /home/hq.user4
  Login shell: /bin/bash
  Principal name: hq.user4@AU.TEAM
  Principal alias: hq.user4@AU.TEAM
  Email address: hq.user4@au.team
  UID: 235400006
  GID: 235400006
  Account disabled: False
  Password: True
  Member of groups: ipausers
  Kerberos keys available: True
[root@srv-hq ~]# ipa user-mod hq.user5 --password
Password:
Enter Password again to verify:
-----------------------
Modified user "hq.user5"
-----------------------
  User login: hq.user5
  First name: hq.user5
  Last name: hq.user5
  Home directory: /home/hq.user5
  Login shell: /bin/bash
  Principal name: hq.user5@AU.TEAM
  Principal alias: hq.user5@AU.TEAM
  Email address: hq.user5@au.team
  UID: 235400007
  GID: 235400007
  Account disabled: False
  Password: True
  Member of groups: ipausers
  Kerberos keys available: True
[root@srv-hq ~]# id hq.user{1,2,3,4,5}
uid=235400003(hq.user1) gid=235400003(hq.user1) groups=235400003(hq.user1)
uid=235400004(hq.user2) gid=235400004(hq.user2) groups=235400004(hq.user2)
uid=235400005(hq.user3) gid=235400005(hq.user3) groups=235400005(hq.user3)
uid=235400006(hq.user4) gid=235400006(hq.user4) groups=235400006(hq.user4)
uid=235400007(hq.user5) gid=235400007(hq.user5) groups=235400007(hq.user5)
[root@srv-hq ~]#
```

----ПОДКЛЮЧЕНИЕ КЛИЕНТОВ----

apt-get install freeipa-client realmd krb5-kinit bind-utils libbind zip task-auth-freeipa

klist
kinit <user>





10.1.1.2 — DNS FREEIPA

----ПОДКЛЮЧЕНИЕ КЛИЕНТОВ БЕЗ ГРАФИКИ----

----OSPF настройка на RTR-HQ и RTR-BR----

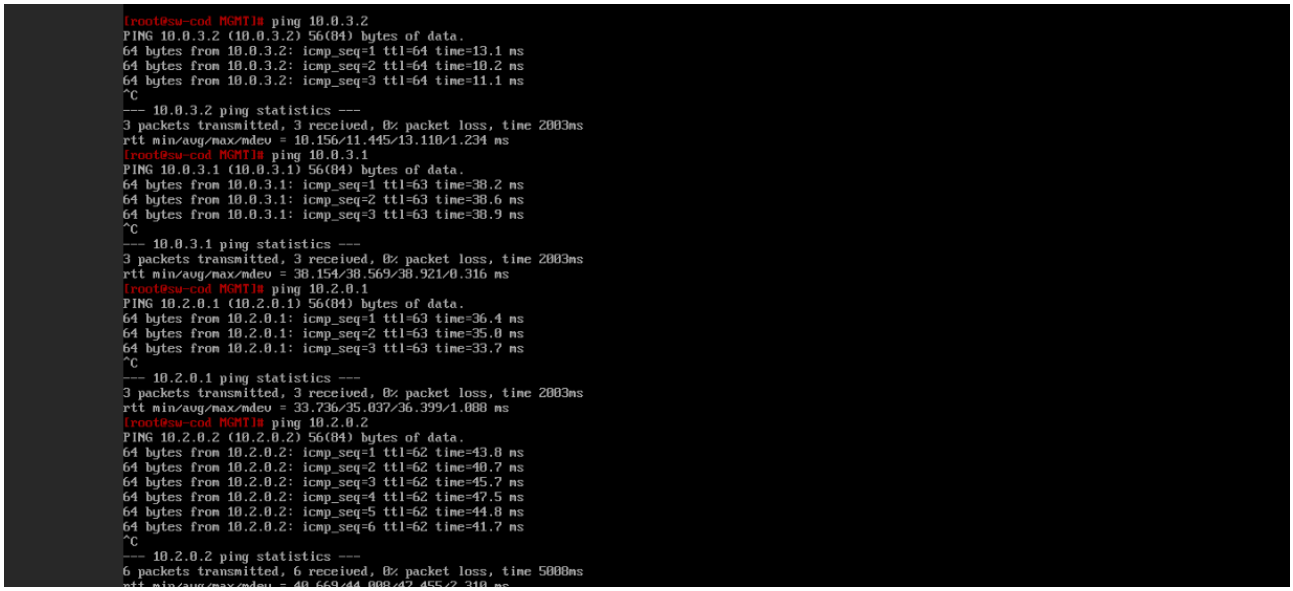
```
rtr-cod>en
rtr-cod#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
rtr-cod(config)#int tunnel.0
rtr-cod(config-if-tunnel)#do sh ip int br
 Interface        IP-Address          Status                VRF
 ---------------------------------------------------------------
 isp              34.95.33.33/24      up                    default
 sw-cod           172.16.0.1/23       up                    default
 tunnel.0         unassigned          down                  default
rtr-cod(config-if-tunnel)#ip address 10.0.3.2/30
rtr-cod(config-if-tunnel)#ip tunnel 84.212.78.78 34.95.33.33 mode gre

2026-03-25 04:15:15      INFO      Interface tunnel.0 changed state to up
rtr-cod(config-if-tunnel)#router ospf 1
rtr-cod(config-router)#router-id 10.0.3.2
rtr-cod(config-router)#passive-interface default
rtr-cod(config-router)#no passive-interface tunnel.0
rtr-cod(config-router)#redistribute static
rtr-cod(config-router)#network 10.3.0/30 area 0
% Invalid network prefix value
rtr-cod(config-router)#network 10.0.3.0/30 area 0
rtr-cod(config-router)#network 172.16.0.0/23 area 0
rtr-cod(config-router)#
```

RCH - Proxmox Console — Mozilla Firefox

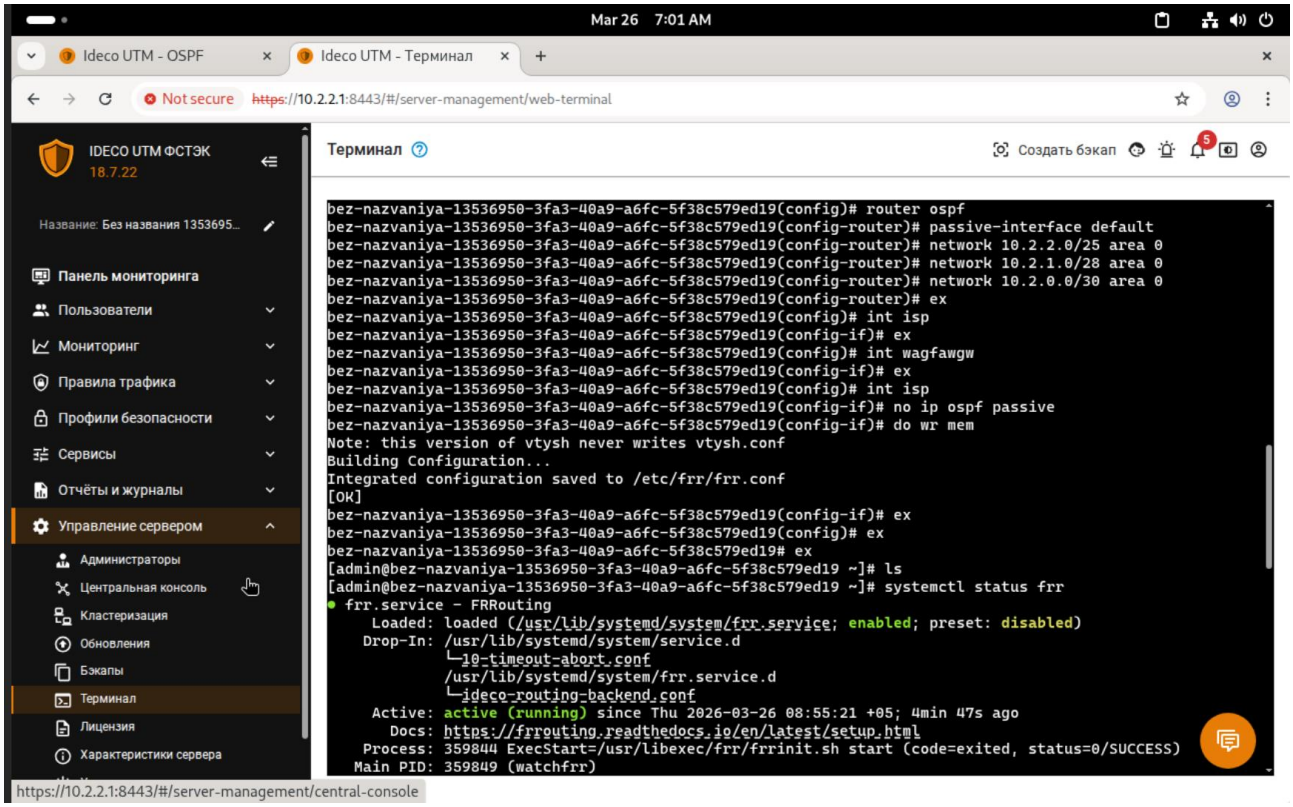
rch.master.local:8006/?console=kvm&xtermjs=1&vmid=2001&vmname=rtr-br&node=RCH&cmd=

```
64 bytes from 34.95.33.33: icmp_seq=1 ttl=63 time=55.0 ms
64 bytes from 34.95.33.33: icmp_seq=2 ttl=63 time=61.7 ms
64 bytes from 34.95.33.33: icmp_seq=3 ttl=63 time=64.0 ms

--- 34.95.33.33 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 55.034/60.253/64.023/3.810 ms
rtr-br(config-if-tunnel)#router ospf 1
rtr-br(config-router)#router-id 10.0.3.1
rtr-br(config-router)#passive-interface default
rtr-br(config-router)#no passive-interface tunnel.0
rtr-br(config-router)#redistribute static
rtr-br(config-router)#do sh ip int br
 Interface        IP-Address          Status                VRF
 ---------------------------------------------------------------
 isp              84.212.78.78/27     up                    default
 fwbr             10.2.0.1/30         up                    default
 tunnel.0         10.0.3.1/30         up                    default
rtr-br(config-router)#network 10.0.3.0/30 area 0
rtr-br(config-router)#network 10.2.0.0/30 area 0
rtr-br(config-router)#
```

Проверка:

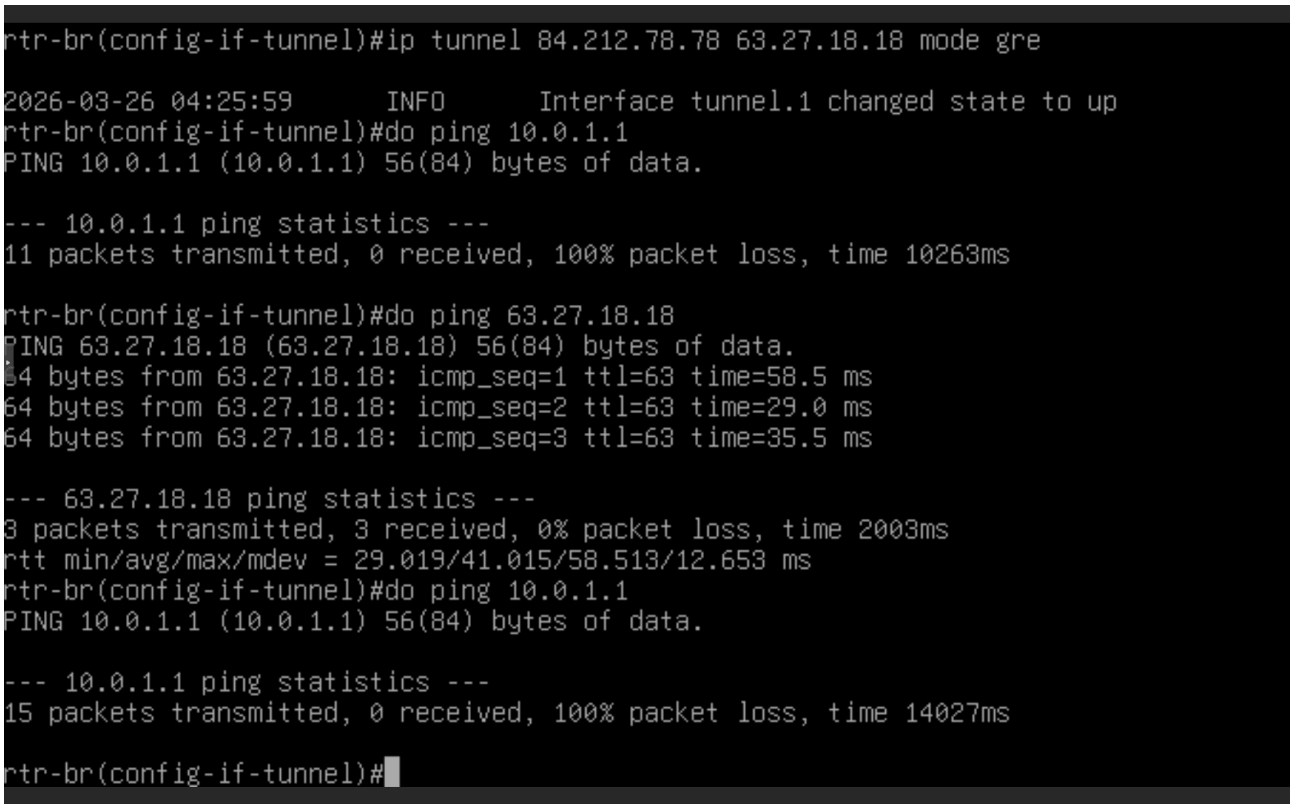


----Настройка OSPF на FW-BR----



----GRE туннель между RTR-BR и FW-HQ----

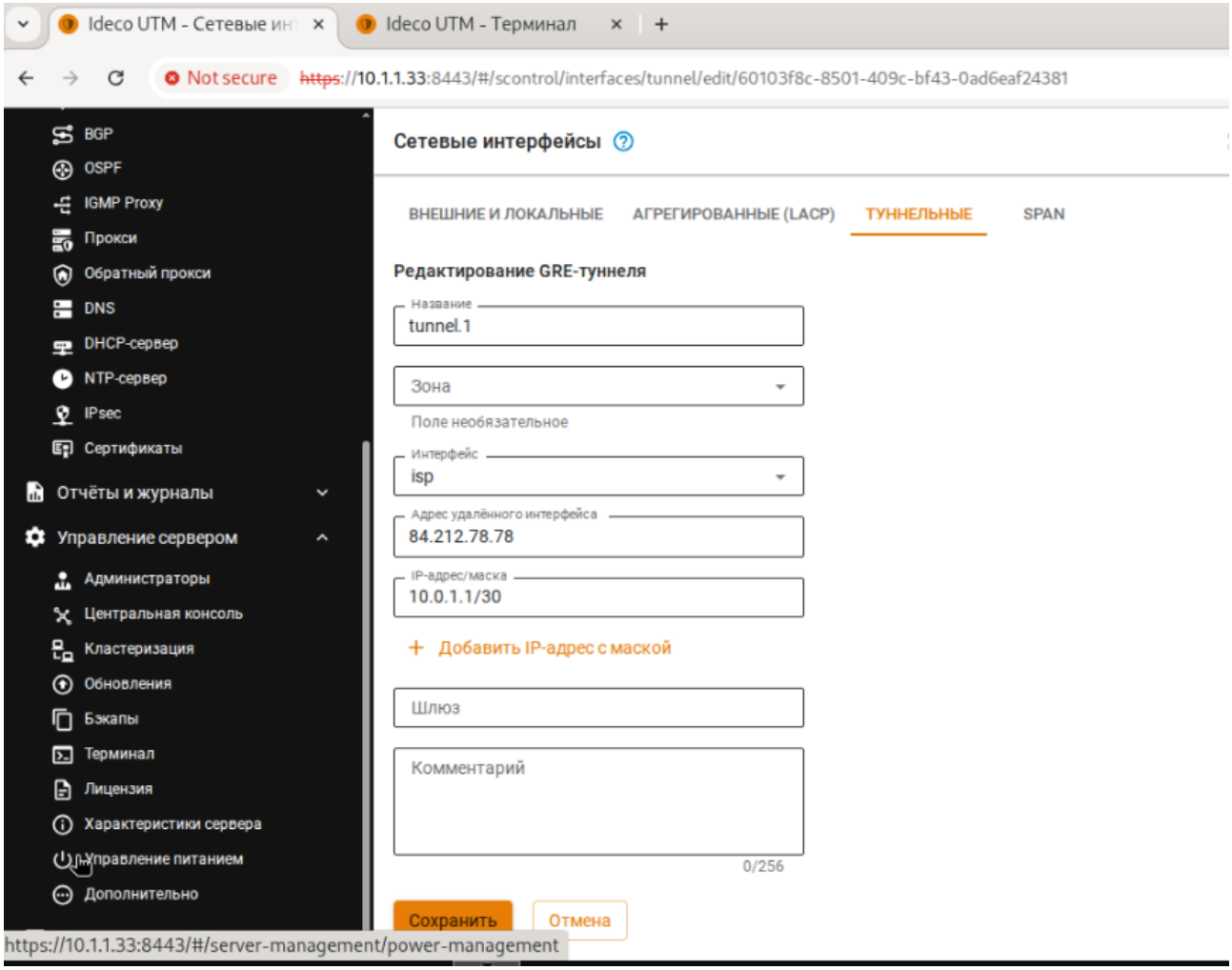
RTR-BR



```
User Access Verification


EcoRouterOS version Camellia 14/05/2024 16:45:56
rtr-br>en
rtr-br#ping 10.0.1.1
PING 10.0.1.1 (10.0.1.1) 56(84) bytes of data.
64 bytes from 10.0.1.1: icmp_seq=1 ttl=64 time=46.9 ms
64 bytes from 10.0.1.1: icmp_seq=2 ttl=64 time=36.9 ms
64 bytes from 10.0.1.1: icmp_seq=3 ttl=64 time=31.6 ms

--- 10.0.1.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 31.590/38.471/46.906/6.348 ms
rtr-br#ping 10.0.1.2
PING 10.0.1.2 (10.0.1.2) 56(84) bytes of data.
64 bytes from 10.0.1.2: icmp_seq=1 ttl=64 time=9.91 ms
64 bytes from 10.0.1.2: icmp_seq=2 ttl=64 time=0.713 ms
64 bytes from 10.0.1.2: icmp_seq=3 ttl=64 time=0.450 ms
64 bytes from 10.0.1.2: icmp_seq=4 ttl=64 time=0.348 ms

--- 10.0.1.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3059ms
rtt min/avg/max/mdev = 0.348/2.855/9.909/4.074 ms
rtr-br#
```

```
interface tunnel.1
 ip mtu 1476
 ip address 10.0.1.2/30
 ip tunnel 84.212.78.78 63.27.18.18 mode gre
!
```

FW-HQ



Остальные туннели аналогично.

Развертка NextCloud (21стр, пункт 9)

----Установка зависимостей----
apt-get update && apt-get install apache2 postgresql15-server nextcloud -y

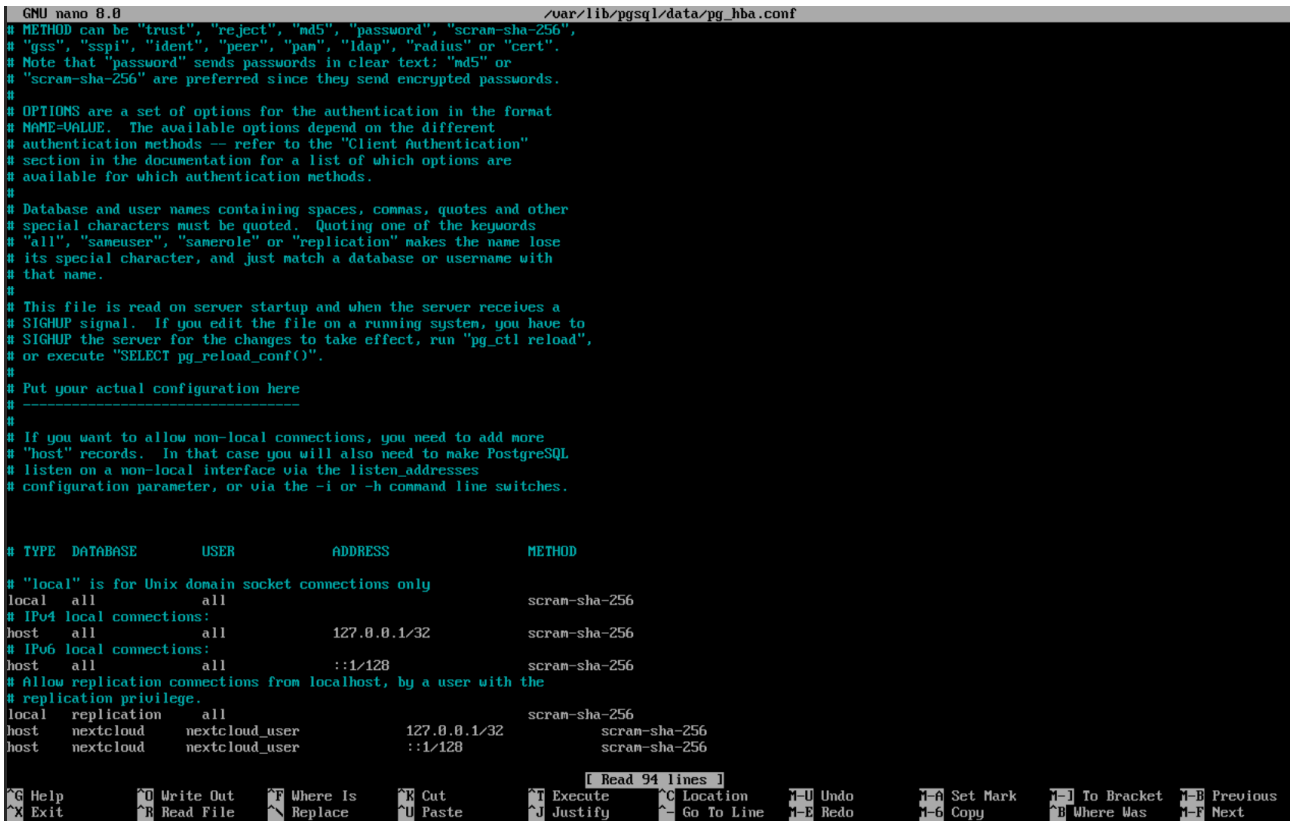
```
/etc/init.d/postgresql initdb

service postgresql start

systemctl enable --now postgresql
```

```
[root@srv-br config]# ip -c a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host proto kernel_lo
       valid_lft forever preferred_lft forever
2: ens18: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether bc:24:11:b4:40:73 brd ff:ff:ff:ff:ff:ff
    altname enp0s18
    inet 10.2.1.2/28 brd 10.2.1.15 scope global ens18
       valid_lft forever preferred_lft forever
    inet6 fe80::be24:11ff:feb4:4073/64 scope link proto kernel_ll
       valid_lft forever preferred_lft forever
[root@srv-br config]# echo "10.2.1.2 ncloud.au.team" >> /etc/host
host.conf    hostname     hosts        hosts.allow  hosts.deny
[root@srv-br config]# echo "10.2.1.2 ncloud.au.team" >> /etc/hosts
[root@srv-br config]#
```

apt-get install -y apache2 postgresql postgresql15-contrib \
php php-pgsql php-gd php-curl php-mbstring php-xml php-zip \
php-bz2 php-intl php-apcu php-imagick php-redis \
libapache2-mod-php certbot python3-module-certbot-apache -y

----Настройка POSTGRESQL----

pqsl -U postgresql



22222222222222222222
apt-get install deploy certbot certbot-apache -y

----Ansible установка----

git clone https://destr.store/admin/ansiblerazvert.git

cd ansiblerazvert

chmod +x
./ansible_razvert.sh

----Ansible настройка доступа----

(AMD-HQ)

ssh-keygen -t rsa -b 2048

ssh-copy-id -f -i /root/.ssh/id_rsa root@ha1-cod.au.team

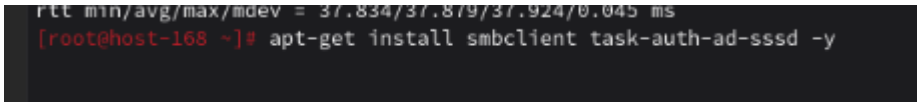
ansible -i inventories/production/hosts -m ping all

ansible-playbook -i inventories/production/hosts playbook2_web.yml

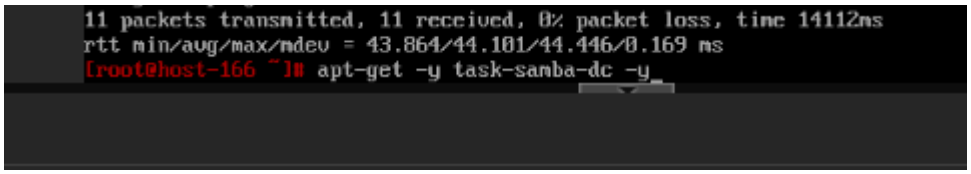
ansible-playbook -i inventories/production/hosts playbook1_web.yml

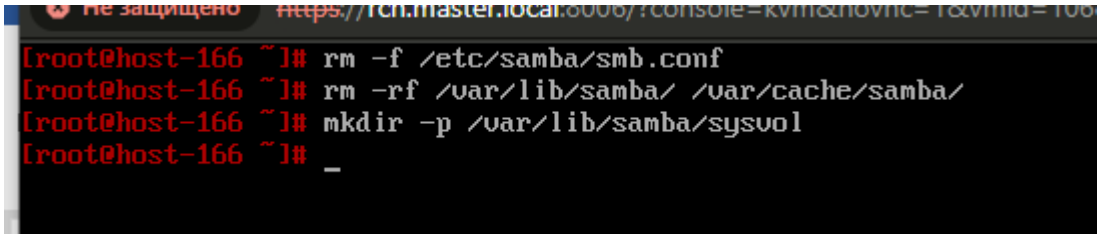
ansible-playbook -i inventories/production/hosts playbook3_web.yml

ALT-LINUX подключение к домену



Установка samba-dc на сервер





Создание копии домена